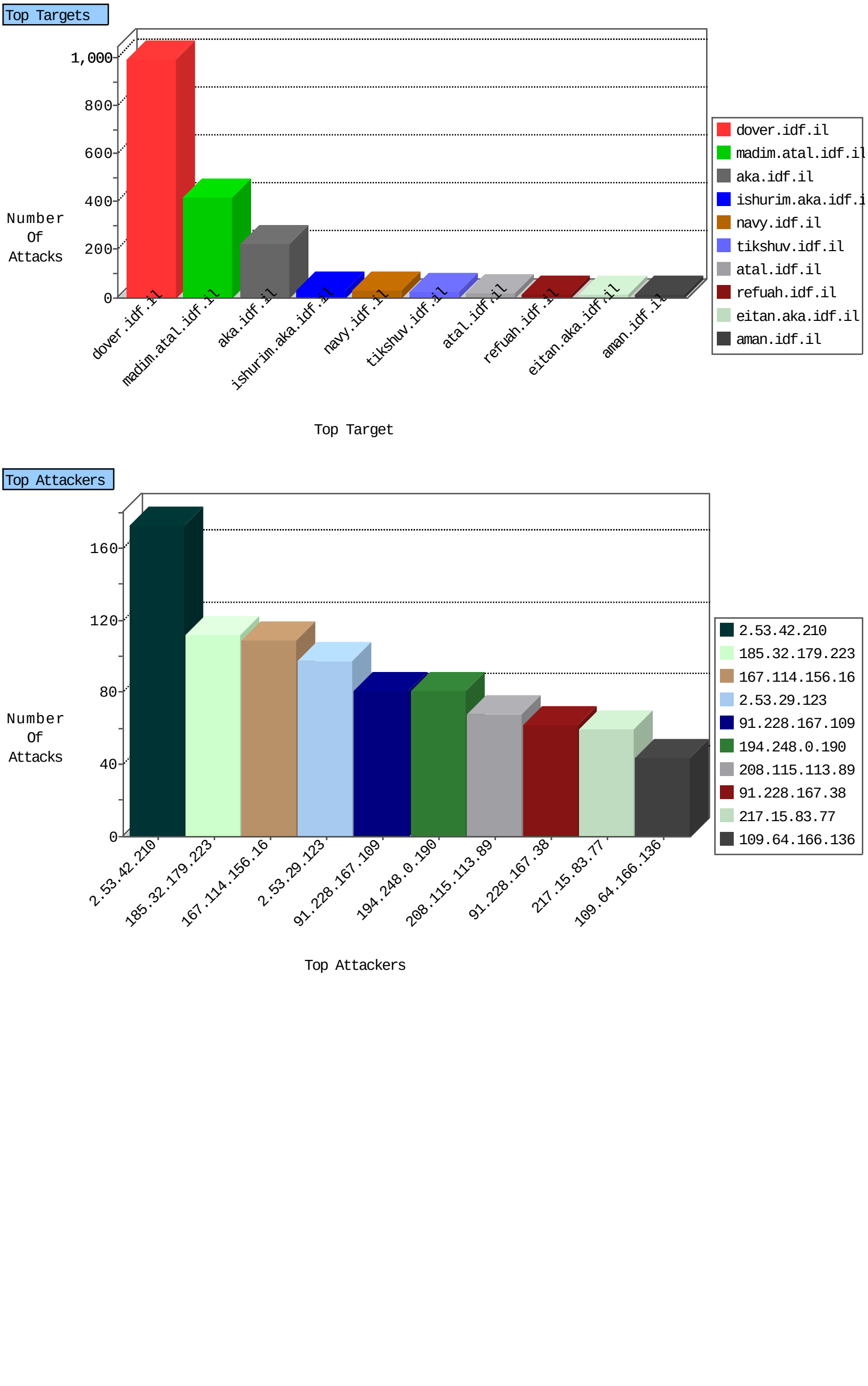
04-27-2016-15:04:04 to 04-27-2016-16:04:04

IDF Under Attack Daily Report



04-27-2016-15:04:04 to 04-27-2016-16:04:04

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	HTTP-POST-Segmented-DoS	dest-reset	3670
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3306
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
192.114.91.211	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
37.117.24.60	Italy	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
94.102.49.116	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
211.108.247.141	Korea, Republic of	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
14.29.32.135	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
94.102.49.116	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

04-27-2016-15:04:04 to 04-27-2016-16:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-27-2016-15:04:04 to 04-27-2016-16:04:04

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
111.119.185.124	147.237.77.216	Pakistan	dover.idf.il	Xenu Link Sleuth User Agent	3
98.119.105.221	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
98.119.105.221	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -f -sS	1
66.240.213.93	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.166.138.159	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
5.141.210.203	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
128.127.0.45	147.237.76.148	Italy	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
104.219.238.10	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
97.78.111.173	147.237.76.30	United States	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.166.138.172	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
13.82.25.17	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
128.127.0.45	147.237.76.148	Italy	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 4096	1

04-27-2016-15:04:04 to 04-27-2016-16:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.248.0.190	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
91.228.167.109	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
91.228.167.38	Slovakia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
217.15.83.77	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
213.61.254.68	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
109.64.166.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
176.13.11.6	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.64.166.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	19
87.70.52.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
5.114.41.137	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
37.26.149.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
128.68.5.235	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
203.133.169.231	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
77.126.12.112	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.3.100.54	Ukraine	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
176.13.4.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
69.22.185.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.66.190	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.114.41.137	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
89.138.71.147	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
50.153.14.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.130.224.22	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
95.150.62.150	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
89.138.71.147	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.39	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.54	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
54.161.102.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.124.29.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
189.79.74.138	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.42.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	173
2.53.29.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
185.32.179.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	93
109.253.136.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
79.178.110.245	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.178.110.245	Block	12
79.183.17.155	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
80.246.133.220	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	3
62.30.2.174	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
149.88.102.68	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/	Block	3
93.47.155.208	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general	Block	2
109.65.208.25	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
46.19.85.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.121.147.167	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
157.55.2.158	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.28.184.8	Israel	147.237.76.147	chinuch.aka.idf.i	PHP Attempt	Block	1
87.71.18.181	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13974-en/dover.aspx&bw=1	Block	1
219.74.36.56	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method ¥ñu.Œæ5É;DH+Z[[#14]]ŠÑœÕNÊä[[#26]]N†ÞA in URL	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
46.116.67.234	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/	Block	1
80.246.133.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
199.30.24.97	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/69059.pdf	Block	1
160.176.38.164	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin	Block	1
5.28.184.8	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
79.177.1.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/newsflash/mobile	Block	1
176.52.44.13	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/'	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/2356.jpg	Block	1
130.185.155.10	Sweden	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
46.117.240.46	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.117.240.46	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/69044.pdf	Block	1
199.30.25.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
65.55.210.100	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
108.26.200.145	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
5.29.58.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
184.105.139.68	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.117.240.46	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/	Block	1
149.78.149.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
2.53.37.217	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.64.66.79	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.231.43	Block	1
199.30.25.93	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
65.55.210.184	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Illegal Byte Code Character in Method ¥ñu.Œæ5É;DH+Z[[#14]]ŠÑœÕNÊä[[#26]]N†ÞA	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
46.118.156.3	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	1