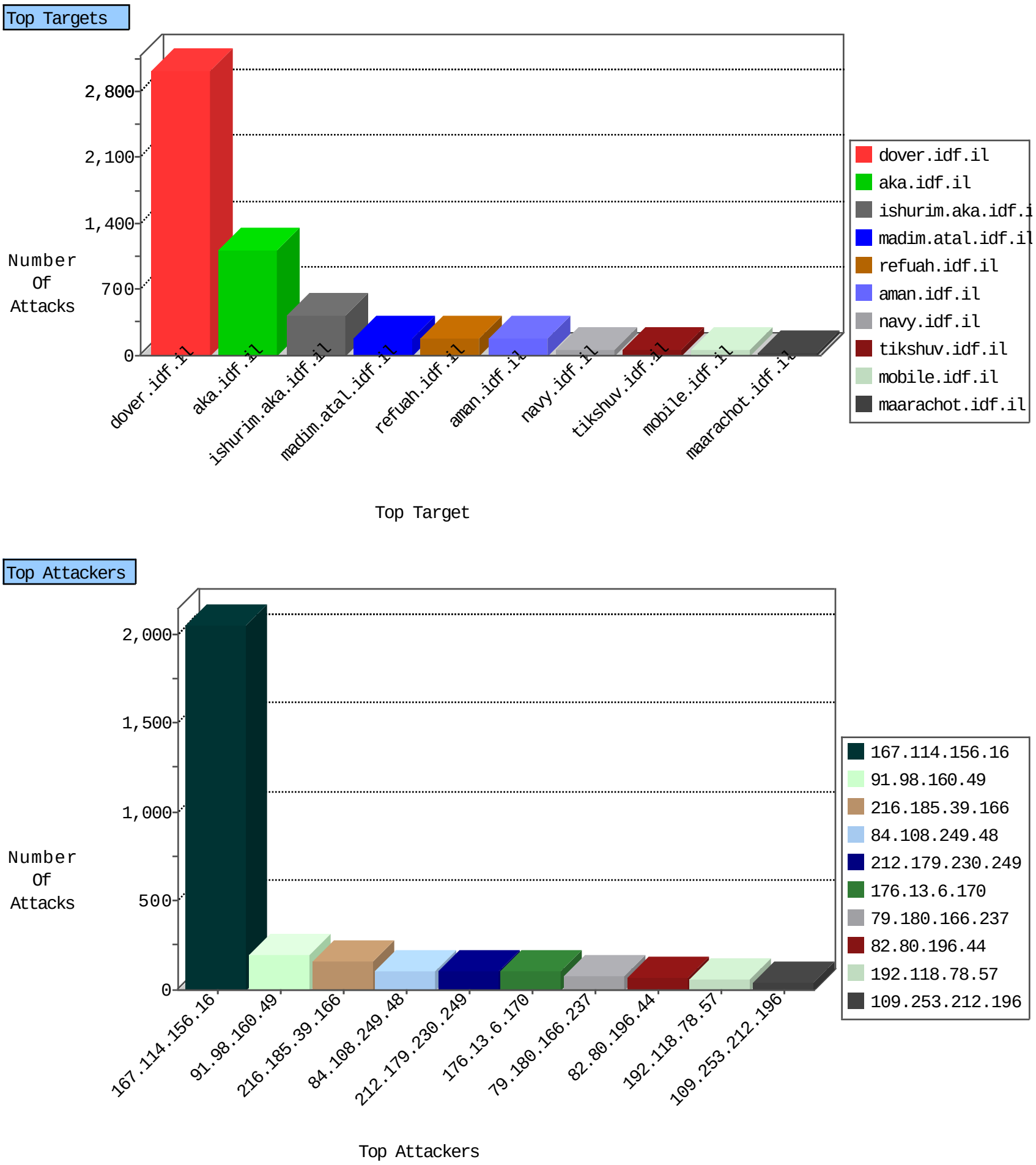
03-15-2016-13:04:06 to 03-15-2016-14:04:06

IDF Under Attack Daily Report



03-15-2016-13:04:06 to 03-15-2016-14:04:06

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	3338
91.98.160.49	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	476
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
82.80.97.80	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	2
159.104.163.17	United Kingdom	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
178.17.170.141	Moldova, Republic of	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1

03-15-2016-13:04:06 to 03-15-2016-14:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.189.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
23.91.70.77	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
67.228.38.74	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
2.54.139.199	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
162.210.196.129	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
2.54.2.166	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.180.135.225	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
108.59.8.80	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.69.79	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-15-2016-13:04:06 to 03-15-2016-14:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.98.160.49	147.237.77.216	Iran, Islamic Republic of	dover.idf.il	ET SCAN NMAP -sS window 1024	9
67.228.38.74	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	9
23.91.70.77	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
85.65.134.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.177.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.197.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.132.48.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.1.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.74	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.165.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.92.72.82	147.237.76.30		himush.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
84.109.53.0	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.95.83.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.129.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.241.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.221	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.125.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-15-2016-13:04:06 to 03-15-2016-14:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
216.185.39.166	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	119
79.180.166.237	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	44
84.108.249.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
109.253.212.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	41
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	38
2.54.186.52	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
84.108.249.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	35
216.185.39.166	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	33
212.179.230.249	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	31
109.67.55.89	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.1.180	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
84.108.249.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	30
82.81.65.6	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
192.118.78.57	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
176.13.1.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.120.57.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
212.179.230.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
176.13.8.123	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
212.179.230.249	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
82.80.193.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
185.32.179.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
109.253.213.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.118.78.57	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
79.183.213.123	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
109.253.215.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.74	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
62.90.220.6	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
79.180.166.237	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
109.253.132.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
80.246.136.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
80.246.136.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
82.80.196.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
212.179.230.249	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.54.162.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
217.194.203.52	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.65.97.37	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.32.179.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
80.246.136.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.54.170.11	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.178.15.223	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.22.131.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
77.125.136.82	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.219.184.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.205	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.120.57.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	11
176.13.19.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
199.203.52.37	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.6.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
109.253.215.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
84.108.84.126	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.108.84.126	Block	14
185.32.179.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.85.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.19.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.116.232.69	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	5
109.253.213.169	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
87.71.94.91	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	3
5.28.158.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.28.158.227	Block	3
80.246.133.126	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.20.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.149.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.116.232.69	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	2
109.65.78.215	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
94.199.238.15	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.53.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.146.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	2
41.40.229.104	Egypt	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
81.218.135.68	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.64.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
31.168.142.114	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/entebbe1.stm<prel=	Block	1
46.116.120.223	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
85.250.203.226	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
212.179.230.249	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
68.180.229.124	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
37.26.148.182	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Open Mode	None	1
185.32.179.114	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.171.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
54.194.68.68	Ireland	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
94.23.40.23	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.116.120.223	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
41.40.229.104	Egypt	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1
82.80.193.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
31.168.142.114	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
46.116.120.223	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
109.65.78.215	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
46.77.124.84	Poland	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.183.8.91	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
37.26.148.191	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
121.169.172.14	Korea, Republic of	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl41 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
46.116.120.223	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
41.40.229.104	Egypt	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/7/size220x0/16037.jpg	Block	1