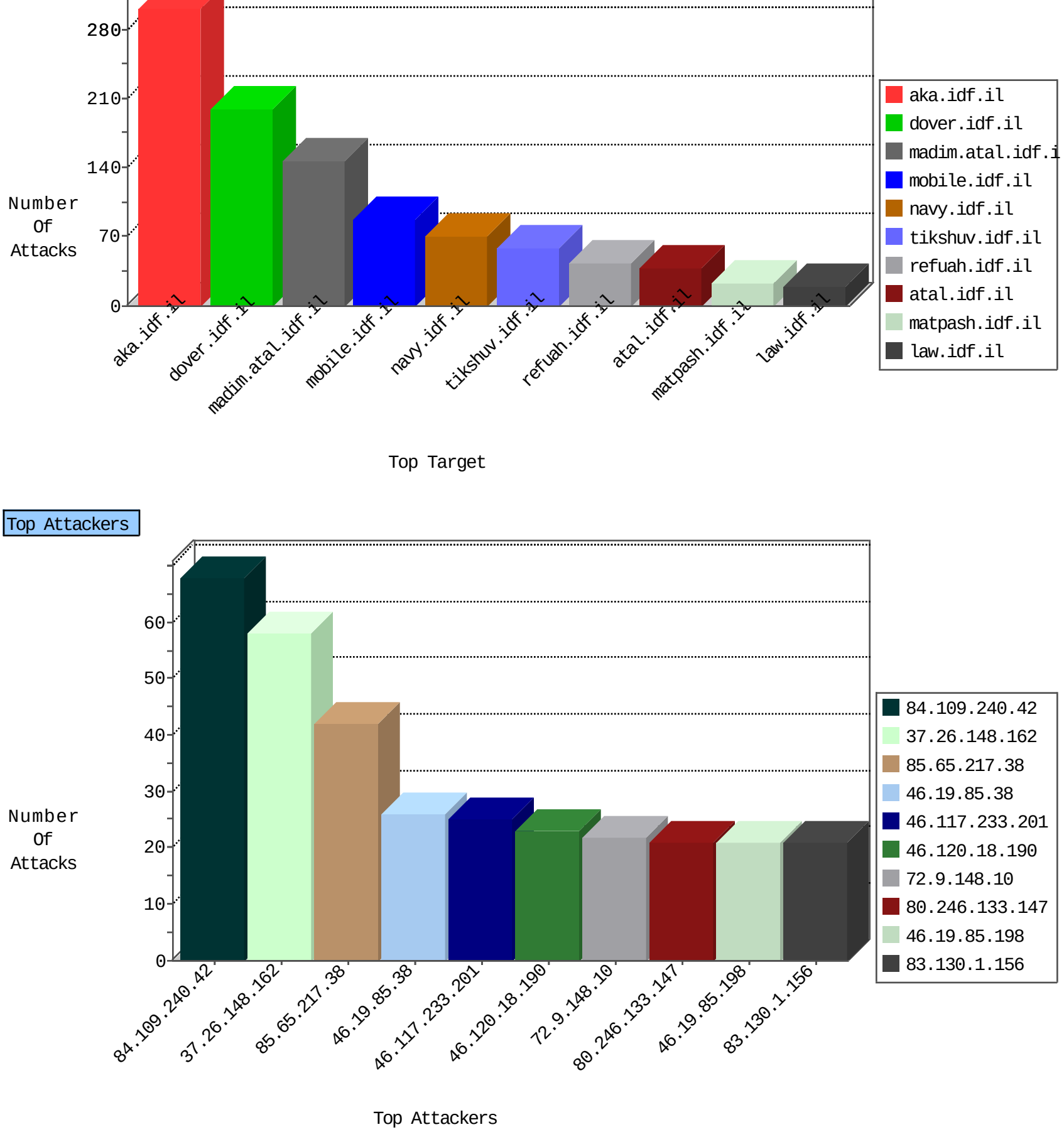
03-08-2016-21:04:03 to 03-08-2016-22:04:03

IDF Under Attack
Daily Report



03-08-2016-21:04:03 to 03-08-2016-22:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
193.81.79.142	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
188.138.17.205	France	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.244	Switzerland	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
217.146.91.36	United Kingdom	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

03-08-2016-21:04:03 to 03-08-2016-22:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.233.201	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	25
132.64.102.76	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.67.104.196	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.54.55.77	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
87.106.179.116	Germany	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
152.115.70.227	Denmark	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3
61.135.189.69	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	3
79.181.187.38	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
83.149.126.98	Netherlands	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
177.185.194.138	Brazil	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
83.149.126.98	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
67.228.38.74	United States	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.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

03-08-2016-21:04:03 to 03-08-2016-22:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
152.115.70.227	147.237.77.74	Denmark	law.idf.il	SQL Injection - Select From	12
177.185.194.138	147.237.76.86	Brazil	navy.idf.il	SQL Injection - Select From	9
67.228.38.74	147.237.77.176	United States	matpash.idf.il	SQL Injection - Select From	6
87.106.179.116	147.237.77.216	Germany	dover.idf.il	SQL Injection - Select From	6
2.54.183.210	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
80.246.130.201	147.237.76.147	Israel	chinuch.aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
213.57.231.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
66.249.69.30	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
80.246.133.147	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
176.13.2.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 2048	1
122.147.148.178	147.237.72.166	Taiwan	aka.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.116.53.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.197.254.53	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
37.1.209.203	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
104.45.210.69	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 3072	1
37.1.209.203	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
94.230.93.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.1.209.203	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.211.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.111.163.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
211.246.162.160	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.253.96.122	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -f -sS	1
104.197.254.53	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
42.159.244.127	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
104.197.254.53	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
37.1.209.203	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
104.45.210.69	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
37.1.209.203	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
84.228.200.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.41.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.246.162.160	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

03-08-2016-21:04:03 to 03-08-2016-22:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
85.65.217.38	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	35
46.120.18.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
109.66.16.97	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
2.52.133.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.203.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.142.142.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
176.13.19.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
83.130.1.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
5.29.62.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.11.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
149.78.18.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.38	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.133.147	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.142.183.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.198	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.102.195.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.198	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
89.138.111.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.109.41	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
195.60.232.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.38	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.96.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.70.13.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.120.125.27		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.133.147	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.130.254.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.172.253.197	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.39.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.46.39.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
83.130.1.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
5.102.254.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.120	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	5
173.12.122.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
80.246.133.147	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
83.130.1.156	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
63.143.34.37	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
80.246.136.35	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
85.130.254.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.204.185	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.179	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.41.181	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.109.240.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
37.26.148.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
5.29.60.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
85.65.217.38	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
37.146.134.221	Russian Federation	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
37.146.134.221	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.146.134.221	Block	5
82.80.157.175	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.52.17.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
86.106.18.51	Romania	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	3
5.29.62.171	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.162	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
5.29.117.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	2
168.221.158.56	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
64.237.45.116	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
37.26.148.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.102.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1108-he/nakhal.aspx	Block	1
207.46.13.99	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 207.46.13.99	Block	1
94.230.93.108	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.26.146.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.55.240	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
173.252.90.237	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
37.26.149.147	Israel	147.237.76.39	mobile.meitav.idf.il	Cookie Tampering on cookie .ASPNETAUTH: Expected 0102423F26FC8947D308FE42B767C78C47D3080009320030003600350030003900340033003200000012F00FF, Observed 010212EC55FA8947D308FE126497C58C47D3080009320030003600350030003900340033003200000012F00FF	None	1
79.178.109.41	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
72.107.211.13	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.230.93.122	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
37.146.134.221	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
79.176.55.240	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
189.69.56.69	Brazil	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.176	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
37.26.149.213	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.133.147	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
77.125.96.192	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
94.230.93.124	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
83.130.1.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.177.61.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.179	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
197.33.47.120	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
37.142.142.99	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
89.138.111.76	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.136.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
79.176.55.240	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
157.55.39.93	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.120.18.190	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
84.108.104.248	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
37.26.148.162	Israel	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.178.1.34	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1