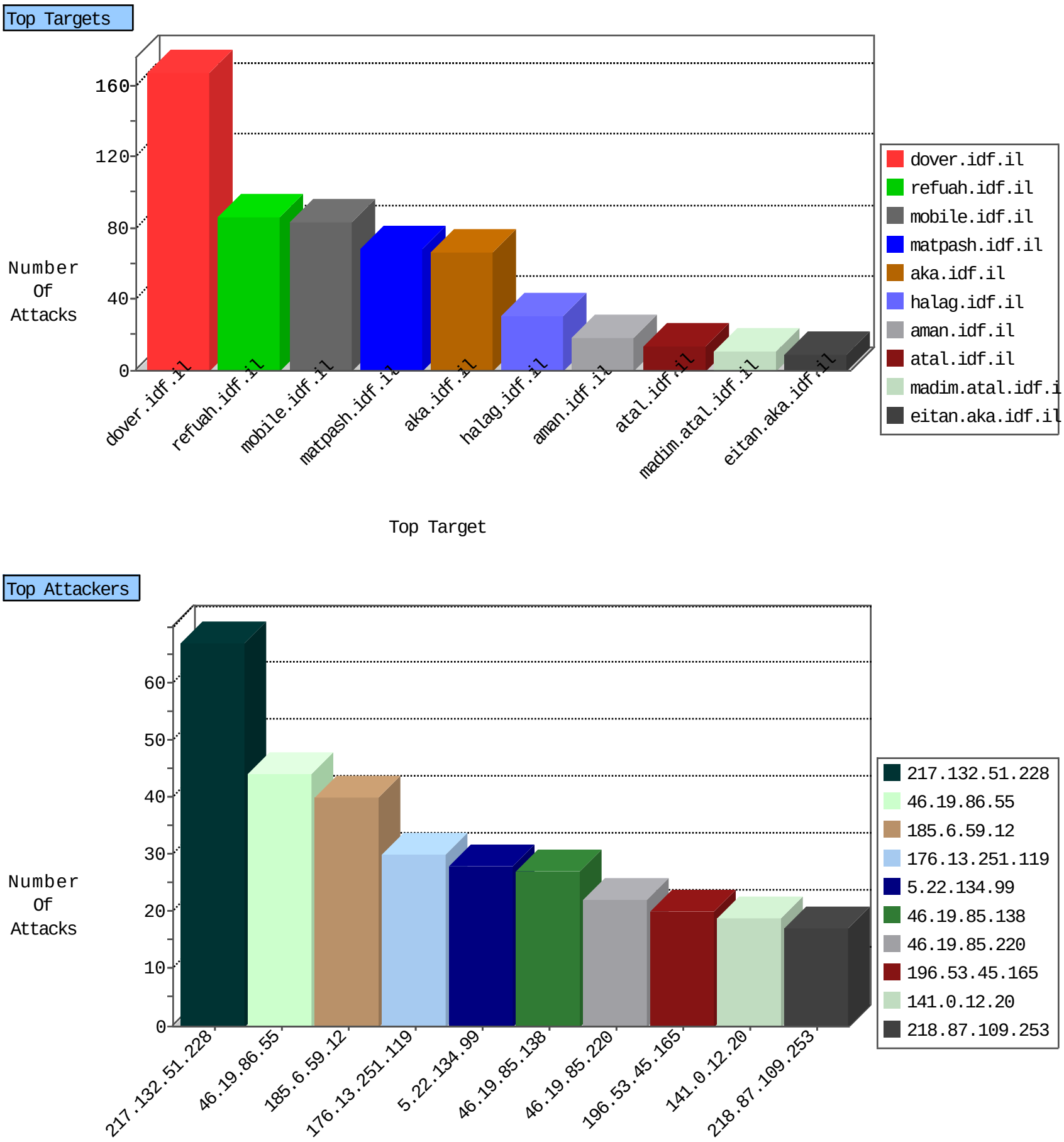
10-01-2016-17:04:02 to 10-01-2016-18:04:02

IDF Under Attack Daily Report



10-01-2016-17:04:02 to 10-01-2016-18:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.249.221.242	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
134.147.203.115	Germany	147.237.76.86	navy.idf.il	Black List	drop	2
196.200.16.201	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
41.206.63.132	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.200.16.203	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
41.206.63.130	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
196.200.16.202	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
41.206.63.133	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
198.167.138.185	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
41.206.63.131	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
196.200.16.202	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
41.206.63.133	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.200.16.201	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
41.206.63.132	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
196.200.16.203	Kenya	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
71.6.146.185	United States	147.237.76.177	ncore.idf.il	Black List	drop	1

10-01-2016-17:04:02 to 10-01-2016-18:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-01-2016-17:04:02 to 10-01-2016-18:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
218.87.109.253	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
192.169.7.91	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.176	China	matpash.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.143	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.87.109.253	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
125.65.82.44	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
40.121.139.43	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
202.65.138.2	147.237.77.121	India	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
192.169.7.91	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
184.105.247.231	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
218.87.109.253	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
117.21.248.87	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
89.43.123.180	147.237.77.243	Romania	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.87.109.253	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
14.152.59.11	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1

10-01-2016-17:04:02 to 10-01-2016-18:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
217.132.51.228	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	66
176.13.251.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.6.59.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.85.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
141.0.12.20	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
196.53.45.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
141.0.15.226	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
79.176.54.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.55	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.86.55	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.86.55	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
84.229.77.16	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
37.26.147.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
185.3.147.231	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.116.75.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.6.59.12	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.37.67.148	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
79.183.65.15	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.234.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
79.181.106.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.3.147.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.21.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.124.8.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.6.59.12	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence		monitor	3
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
185.3.147.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.219	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.124.42.230	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.3.147.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.108.126.13	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.65.21	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	2
46.19.85.208	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.46.41.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.204.215	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
77.138.22.113	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.164	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.6.59.12	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.224.14	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
79.181.106.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.138.140.248	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
46.121.146.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.2.159	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.139.120	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.124.8.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
23.250.3.10	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
188.37.209.11	Portugal	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-en/	Block	1
157.55.39.161	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
46.116.75.14	Israel	147.237.77.243	mobile.idf.il	Illegal HTTP Version	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
89.237.86.23	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
77.138.183.144	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
207.46.13.30	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
46.242.78.44	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
83.77.252.251	Switzerland	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1249-he/atal.aspx	Block	1
46.116.75.14	Israel	147.237.77.243	mobile.idf.il	Malformed URL en-us	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	NULL Character in URL	Block	1
109.66.182.141	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
77.138.243.23	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
217.132.51.228	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.102.6.30	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple NULL Character in Method from 169.229.3.91	Block	1
84.229.77.16	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.22.113	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	1
46.116.75.14	Israel	147.237.77.243	mobile.idf.il	Multiple Abnormally Long Request from 46.116.75.14	Block	1
185.32.179.164	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
109.66.187.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyud	Block	1
77.139.241.56	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
66.249.65.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8974-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
85.64.212.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.139.237	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	1
46.116.75.14	Israel	147.237.77.243	mobile.idf.il	Unknown HTTP Request Method Accept-Language: in URL en-us	Block	1
185.120.125.11	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
119.76.78.71	Thailand	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
66.249.65.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8832-he/refuah.aspx	Block	1
46.116.75.14	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Multiple Illegal Byte Code Character in URL from 169.229.3.91	Block	1
87.69.122.129	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1

10-01-2016-17:04:02 to 10-01-2016-18:04:02