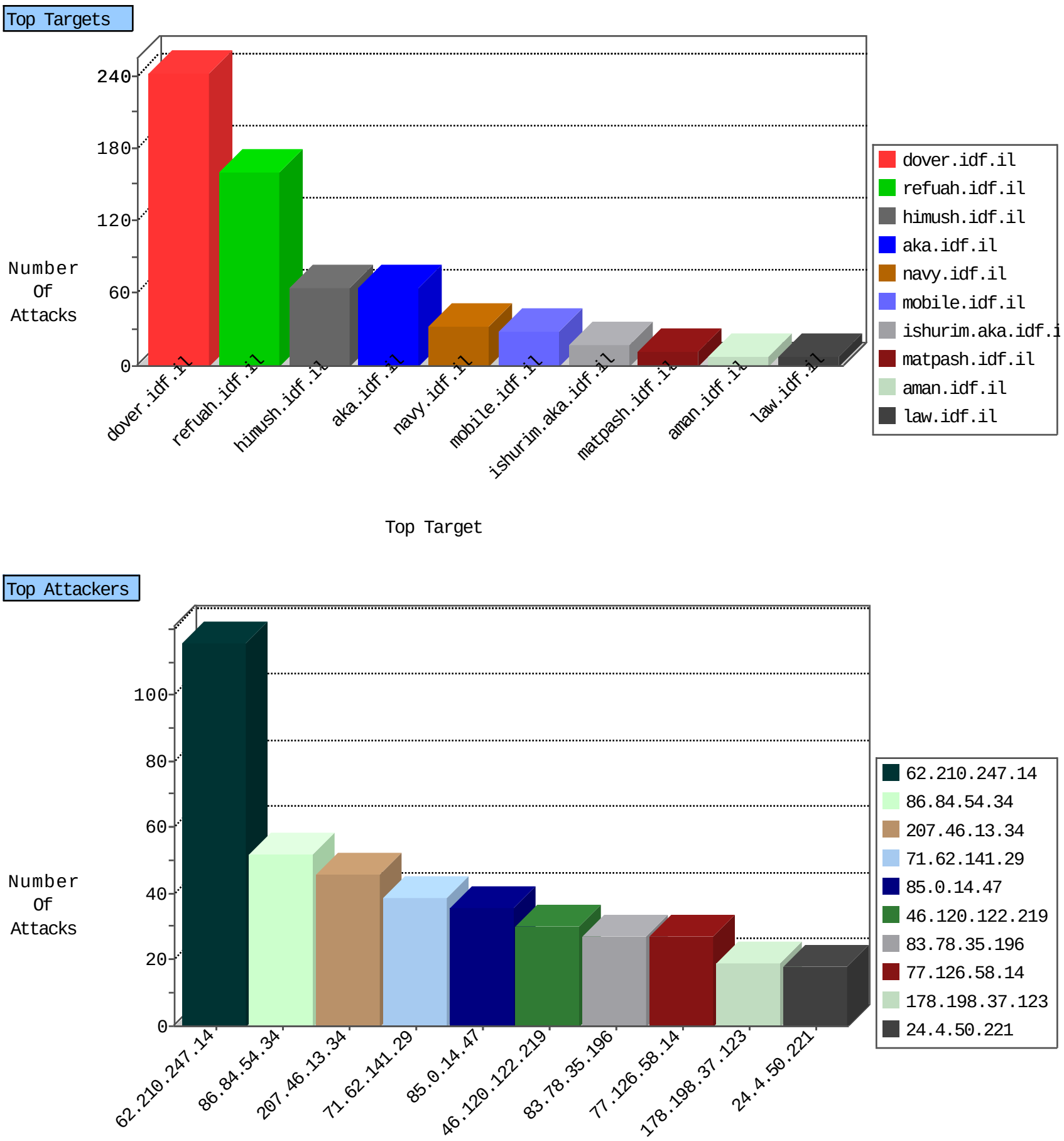
10-02-2016-23:11:57 to 10-03-2016-00:11:57

IDF Under Attack
Daily Report



10-02-2016-23:11:57 to 10-03-2016-00:11:57

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
180.97.106.37	China	147.237.76.196	e.sviva.idf.il	Black List	drop	1
191.96.249.49	Chile	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

10-02-2016-23:11:57 to 10-03-2016-00:11:57

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.247.14	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	114
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3
62.210.247.14	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-02-2016-23:11:57 to 10-03-2016-00:11:57

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	29
117.5.148.240	147.237.77.216	Vietnam	dover.idf.il	Xenu Link Sleuth User Agent	4
117.158.160.211	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
106.75.9.82	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
159.203.101.193	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
159.203.101.193	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential SSH Scan	1
159.203.101.193	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
75.146.164.205	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.82.44	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
125.65.82.44	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.18.95.71	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
117.158.160.211	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.116.57.197	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.18.95.71	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
117.158.160.211	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
159.203.101.193	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
159.203.101.193	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
159.203.101.193	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential SSH Scan	1
159.203.101.193	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
125.65.82.44	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.18.95.71	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
125.65.82.44	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.18.95.71	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
117.158.160.211	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

10-02-2016-23:11:57 to 10-03-2016-00:11:57

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
86.84.54.34	Netherlands	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	52
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	42
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.55.47.170	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
71.62.141.29	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	8
71.62.141.29	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
2.53.134.185	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
71.62.141.29	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	7
71.62.141.29	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	7
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.233	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	7
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
71.62.141.29	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.141.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.26.146.130	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
24.4.50.221	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
52.3.127.144	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	5
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
46.219.211.15	Ukraine	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.202.44	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
50.100.95.169	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.143	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
46.19.85.143	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
87.71.10.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
77.139.211.201	France	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
109.253.202.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.130.5	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.136	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
177.228.67.201	Mexico	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.136	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
50.100.95.169	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
24.4.50.221	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2

10-02-2016-23:11:57 to 10-03-2016-00:11:57

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	2
46.120.69.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.54	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1489-he/atal.aspx	Block	1
77.139.26.34	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
66.249.65.10	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
40.77.167.92	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
77.139.90.81	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
79.183.39.16	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.52	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.29.181.69	Block	1
204.79.180.163	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2061-he/cogat.aspx	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
84.111.114.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
66.249.65.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8819-he/refuah.aspx	Block	1
5.29.181.69	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
204.79.180.183	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
75.85.70.23	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/chinuch/home/default.asp	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
92.8.33.103	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133	Block	1
66.249.66.105	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1

10-02-2016-23:11:57 to 10-03-2016-00:11:57