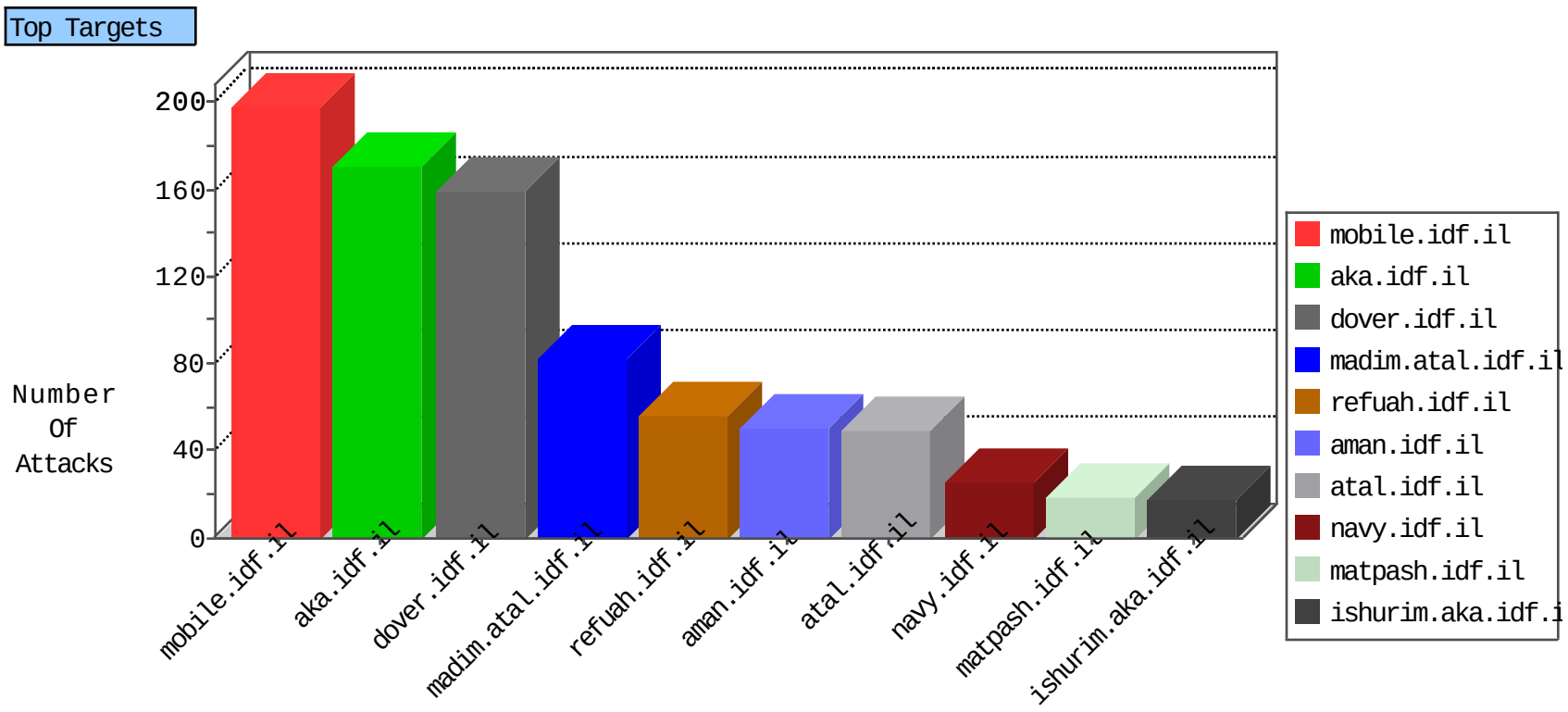
09-01-2016-14:04:08 to 09-01-2016-15:04:08

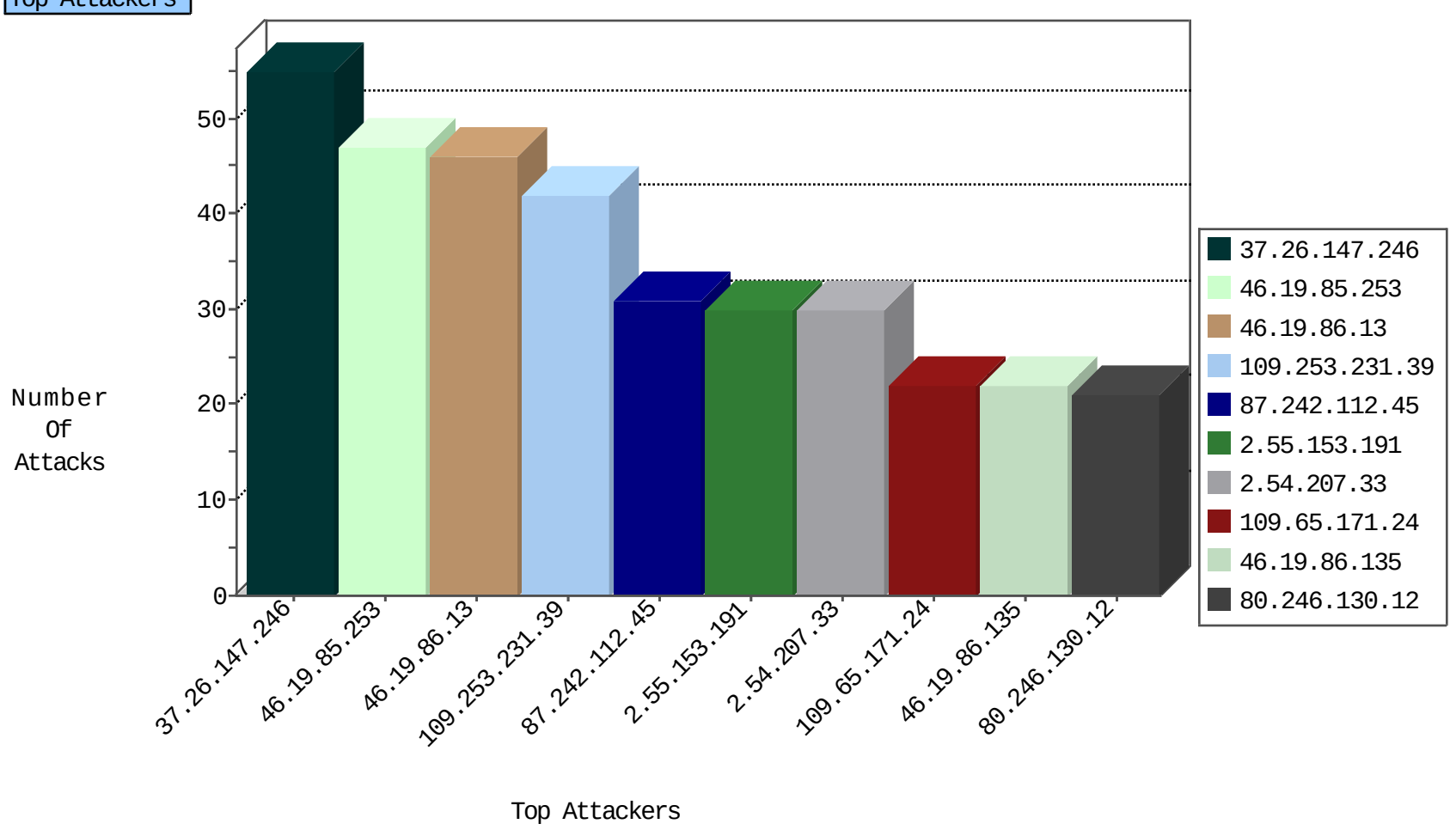
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-01-2016-14:04:08 to 09-01-2016-15:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.160.242.40	Israel	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	3
5.189.186.243	Germany	147.237.76.44	e.refuah.idf.il	Black List	drop	2
5.189.186.243	Germany	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
5.189.186.243	Germany	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	2
5.189.186.243	Germany	147.237.76.176	test.ncore.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.197	e.himush.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.201	e.atal.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.44	e.refuah.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.42	refuah.idf.il	Black List	drop	1

09-01-2016-14:04:08 to 09-01-2016-15:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.242.112.45	Russian Federation	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
87.242.112.45	Russian Federation	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
83.168.250.50	Sweden	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.242.112.45	Russian Federation	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
87.242.112.45	Russian Federation	147.237.76.42	refuah.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-01-2016-14:04:08 to 09-01-2016-15:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
87.242.112.45	147.237.76.42	Russian Federation	refuah.idf.il	SQL Injection - Select From	13
83.168.250.50	147.237.77.216	Sweden	dover.idf.il	SQL Injection - Select From	6

09-01-2016-14:04:08 to 09-01-2016-15:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.231.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.55.153.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.207.33	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.65.171.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
80.246.130.12	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
37.26.147.246	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
192.114.1.131	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
46.19.86.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
80.246.137.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	14
89.237.114.119	France	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.196.9	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
46.19.86.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.53.29.137	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
37.26.147.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
2.53.42.76	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	8
46.19.86.13	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.149.131	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.149.131	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
37.26.147.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
109.253.158.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.230.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.138.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.81.12.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.12.196	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.193	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.22.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.191.142	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.55.189.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.92.43.120		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.147.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.85.67	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
37.26.147.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.32.179.30	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
177.12.172.43	Brazil	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
176.13.6.186	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.85.7	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
199.203.108.153	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.13	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.185.204.63	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.210.174.59	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.211	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
62.0.222.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.66.136.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
46.19.85.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
80.246.137.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.231.39	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.207.33	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
2.55.153.191	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
213.57.48.83	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	5
213.57.48.83	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	4
77.139.171.248	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	3
46.19.86.13	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	3
89.237.114.119	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
65.55.210.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.148.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
199.30.25.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.122	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.111.152.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.43.198	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.29	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
65.55.210.201	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.179.245.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
80.246.138.124	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.201	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.71.63.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.88	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.55.189.106	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
199.30.24.224	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.13.1.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.55.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.139.102.129	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.139.102.129	Block	1
180.76.15.141	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1
82.81.12.31	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
46.19.86.135	Israel	147.237.77.233	atal.idf.il	Illegal HTTP Version	Block	1
176.13.12.196	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
95.221.223.11	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
2.53.191.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
185.89.217.234	Netherlands	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../images/shared/home.png	Block	1
141.226.162.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sacar	Block	1
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
46.19.86.135	Israel	147.237.77.233	atal.idf.il	Malformed URL safari/601.1	Block	1
176.13.22.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
105.104.20.184	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
216.244.66.241	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
141.226.217.243	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.150.128	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.138.246.255	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/edim/yoman/yoman.asp	Block	1
46.19.86.135	Israel	147.237.77.233	atal.idf.il	Unknown HTTP Request Method E238 in URL safari/601.1	Block	1
176.13.230.100	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.65.171.24	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1