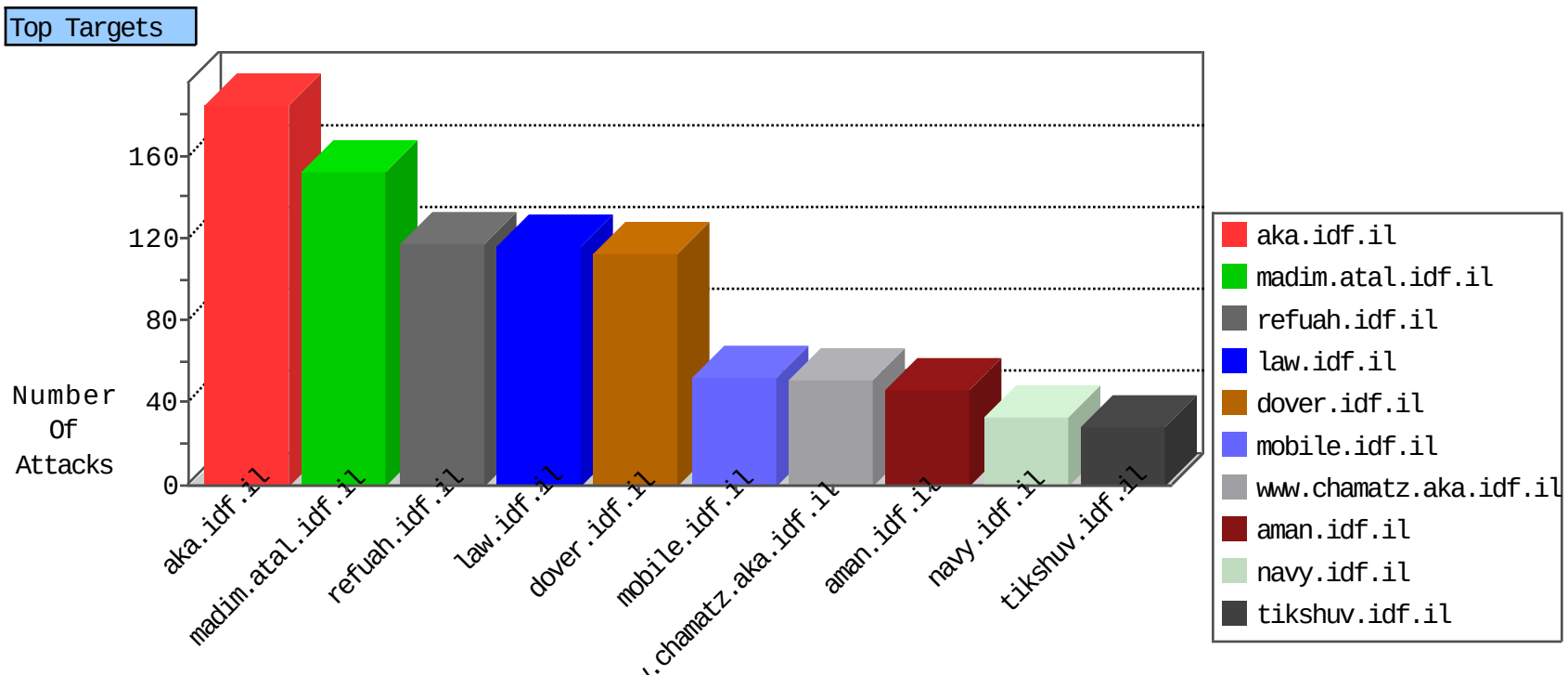
09-04-2016-23:04:08 to 09-05-2016-00:04:08

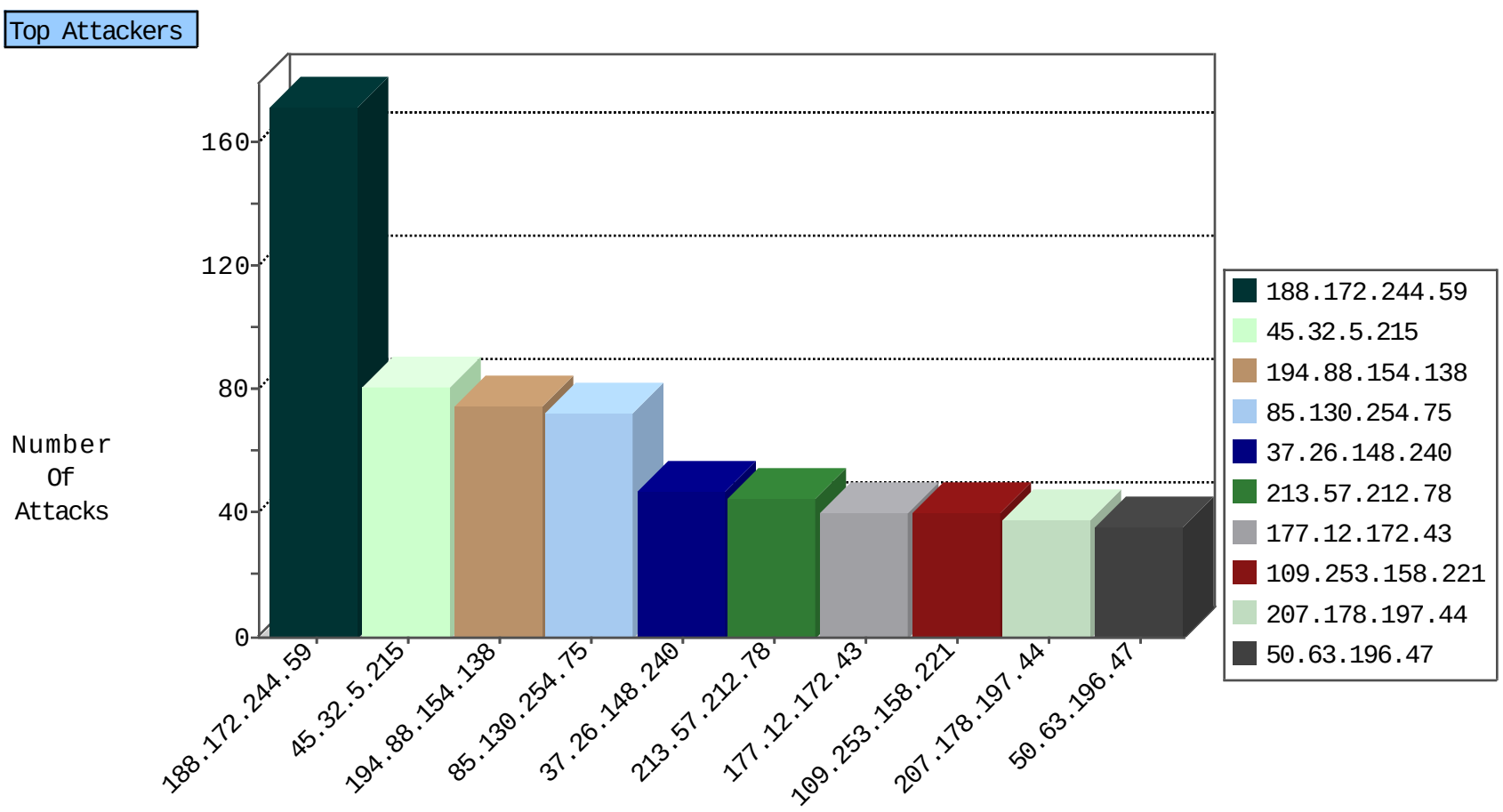
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-04-2016-23:04:08 to 09-05-2016-00:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
211.179.56.16	Korea, Republic of	147.237.76.31	nakchal.idf.il	Black List	drop	2
217.23.9.123	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
66.240.236.119	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
123.59.59.52	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1

09-04-2016-23:04:08 to 09-05-2016-00:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.178.197.44	United States	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
50.63.197.9	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
81.88.48.113	Italy	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
194.88.154.138	Poland	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
62.149.132.252	Italy	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.12.172.43	Brazil	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.29.211.141	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
177.12.172.43	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.96.128.60	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
194.88.154.138	Poland	147.237.76.42	refuah.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
207.178.197.44	United States	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
194.88.154.138	Poland	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.147.117.51	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
72.167.131.75	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
199.58.86.211	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.211	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
50.63.196.47	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
50.63.196.47	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

09-04-2016-23:04:08 to 09-05-2016-00:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
194.88.154.138	147.237.76.42	Poland	refuah.idf.il	SQL Injection - Select From	57
207.178.197.44	147.237.77.226	United States	www.chamatz.aka.idf.il	SQL Injection - Select From	20
66.29.211.141	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	18
209.147.117.51	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	15
177.12.172.43	147.237.72.166	Brazil	aka.idf.il	SQL Injection - Select From	14
177.12.172.43	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	14
66.96.128.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
62.149.132.252	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	8
81.88.48.113	147.237.72.166	Italy	aka.idf.il	SQL Injection - Select From	8
50.63.197.9	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
50.63.196.47	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
50.63.196.47	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	3
72.167.131.75	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	2
221.175.34.145	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
50.116.123.135	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
188.27.238.91	147.237.76.30	Romania	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.227.67.172	147.237.76.202	Sweden	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
122.100.245.78	147.237.76.38	Macau	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.86.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.69.28	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
50.116.123.135	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
149.56.144.220	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.172.71.251	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

09-04-2016-23:04:08 to 09-05-2016-00:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.254.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
85.130.254.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	24
50.63.196.47	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
85.130.254.75	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
109.253.220.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
209.17.114.79	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	18
188.172.244.59	Austria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
188.172.244.59	Austria	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
188.172.244.59	Austria	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
2.53.134.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
188.172.244.59	Austria	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
188.172.244.59	Austria	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
188.172.244.59	Austria	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
188.172.244.59	Austria	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
192.187.101.170	United States	147.237.72.14	dover.idf.il(old)	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
79.188.165.62	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
106.39.60.189	China	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	8
188.172.244.59	Austria	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
188.172.244.59	Austria	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
84.110.177.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
185.112.233.187	Iraq	147.237.0.35	akaws.idf.il	drop	First packet isn't SYN	drop	7
188.172.244.59	Austria	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
84.110.177.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.188.165.62	Poland	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
45.32.5.215	Netherlands	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
188.172.244.59	Austria	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
83.168.250.50	Sweden	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
188.172.244.59	Austria	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
66.96.128.60	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
79.188.165.62	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
176.13.224.36	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.12.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.139.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
184.168.27.116	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
188.172.244.59	Austria	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
50.63.196.47	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.172.244.59	Austria	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.172.244.59	Austria	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
106.39.60.184	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
45.32.5.215	Netherlands	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.172.244.59	Austria	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.172.244.59	Austria	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
45.32.5.215	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.172.244.59	Austria	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
188.172.244.59	Austria	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
66.249.81.179	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
188.172.244.59	Austria	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
45.32.5.215	Netherlands	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

09-04-2016-23:04:08 to 09-05-2016-00:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.212.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
37.26.148.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
109.253.158.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
2.53.14.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
37.26.149.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
141.226.161.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.74.190	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
176.13.224.36	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.139.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version _pk_ses.20.8afc=*	Block	1
213.174.99.140	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	1
109.253.193.213	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
192.198.151.43	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/portalmiluim/templates/home.asp	Block	1
89.138.139.62	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=18a6eac3d341f203.1471462269.2.1473020612.1473020612.;	Block	1
2.53.12.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
37.142.222.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
207.46.13.76	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/www.behazdaa.org.il	Block	1
93.172.204.101	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method D7%A4%D7%95%D7%9F%26gs_l%3Dmobile-gws-serp.1.0.0i71k1l5.0.0.0.1773.0.0.0.0.0.0.0.0..0.0....0...1..64.mobile-gws-serp..0.0.0.QviXMMDpiRQ%22%5D; in URL _pk_id.20.8afc=18a6eac3d341f203.1471462269.2.1473020612.1473020612.	Block	1
171.48.122.40	India	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
67.225.24.91	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
40.77.167.83	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
213.57.204.187	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
93.172.204.101	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 93.172.204.101	Block	1
63.155.175.50	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.21.254	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
79.178.33.57	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
46.19.85.217	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1

09-04-2016-23:04:08 to 09-05-2016-00:04:08