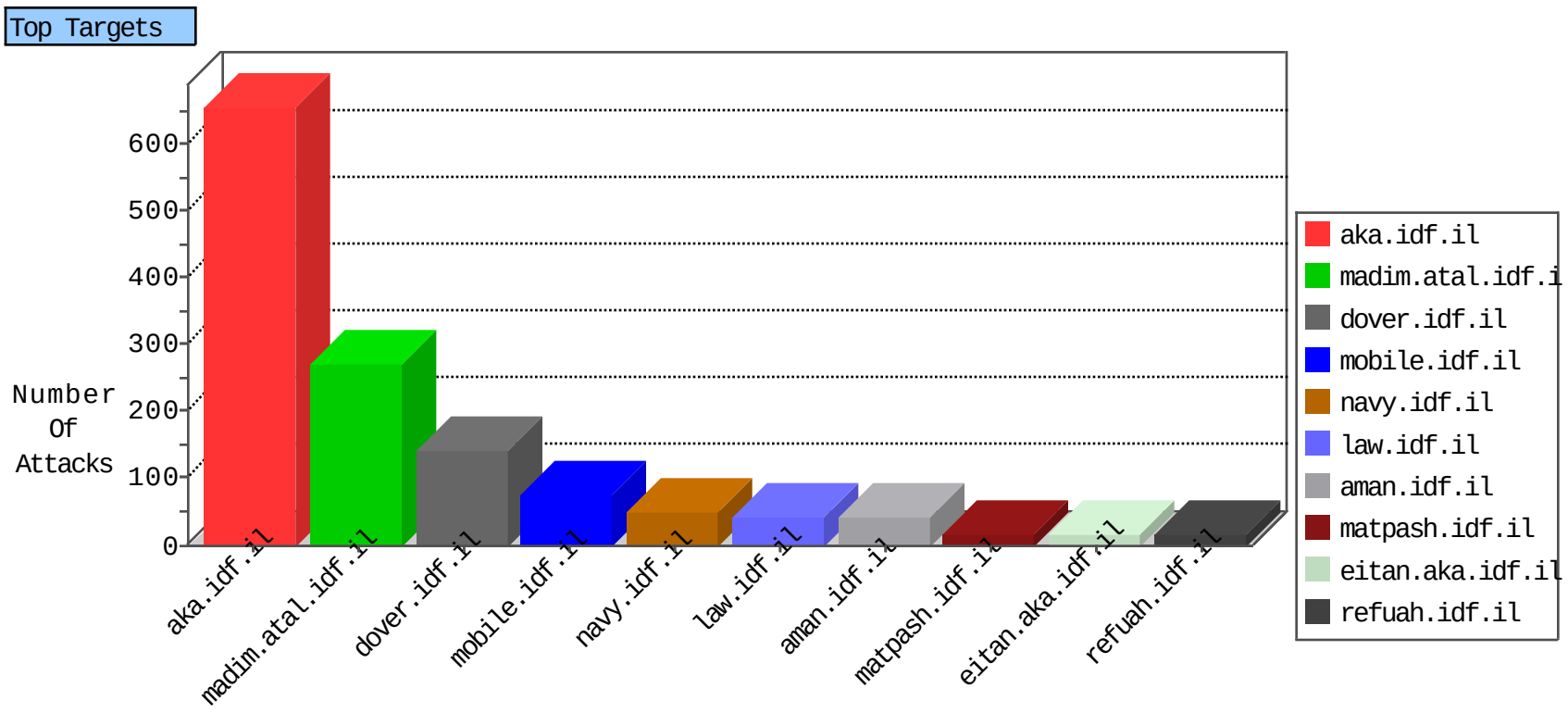
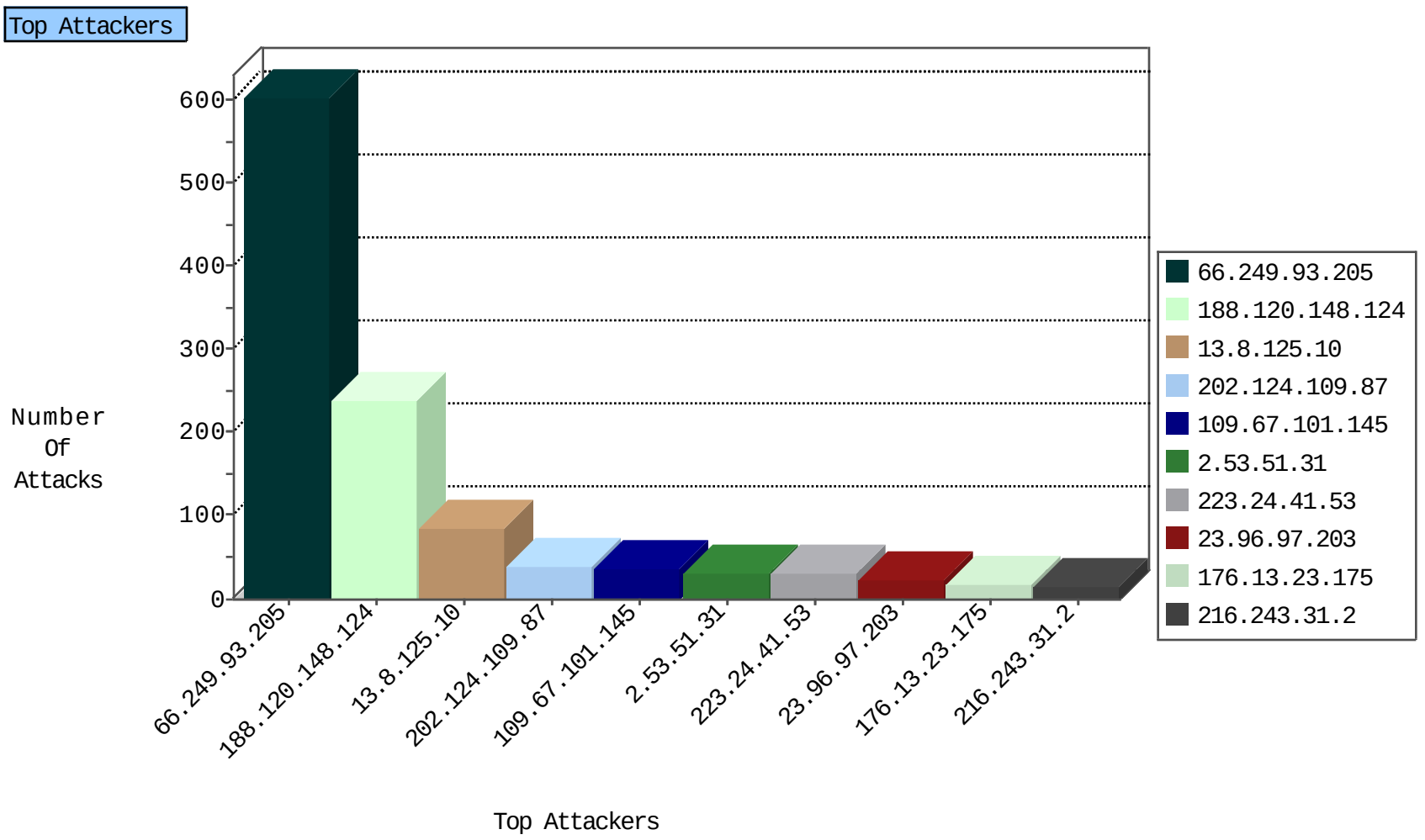
09-23-2016-19:04:05 to 09-23-2016-20:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-23-2016-19:04:05 to 09-23-2016-20:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.117.10.226	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
198.204.224.236	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
69.30.193.252	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
198.204.224.236	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
69.30.193.254	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
198.204.224.235	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
69.30.193.252	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
204.12.220.85	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
142.54.174.86	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	1
204.12.220.85	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
173.208.197.202	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
208.110.84.67	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
63.141.231.211	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
204.12.220.82	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
69.30.227.222	United States	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
221.212.73.37	China	147.237.72.166	aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-23-2016-19:04:05 to 09-23-2016-20:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
202.124.109.87	New Zealand	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
202.124.109.87	New Zealand	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.96.97.203	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
202.124.109.87	New Zealand	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	5
23.96.97.203	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.96.97.235	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
174.34.135.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
23.96.97.238	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
23.96.97.233	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
23.96.97.233	United States	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1
23.96.97.235	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

09-23-2016-19:04:05 to 09-23-2016-20:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.205	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	604
202.124.109.87	147.237.76.86	New Zealand	navy.idf.il	SQL Injection - Select From	19
23.96.97.203	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	12
23.96.97.235	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	5
23.96.97.233	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	2
184.168.80.49	147.237.72.166	United States	aka.idf.il	Tehila - Perl LWP with fake user agent	2
109.65.193.85	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
185.129.148.230	147.237.8.46	Latvia	e.chinuch.idf.i	ET SCAN NMAP -sS window 1024	1
163.172.238.45	147.237.77.216	United Kingdom	dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
23.96.97.238	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	1
14.134.10.3	147.237.77.216	China	dover.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

09-23-2016-19:04:05 to 09-23-2016-20:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
13.8.125.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
109.67.101.145	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	36
223.24.41.53	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.51.31	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
188.247.72.63	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
37.26.149.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.172.153.47	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.66.19.149	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
2.53.143.180	Israel	147.237.76.200	eitan.aka.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
46.19.85.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.142.2.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
84.108.32.214	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.3.147.208	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.64.21.244	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.110.180.77	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
202.124.109.87	New Zealand	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
2.53.20.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.72.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.117.10.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.132.158	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
157.55.39.190	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
213.57.195.133	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
213.8.204.34	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
188.161.112.11	Palestinian Territory Occupied	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.233.85.136	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.154.81.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
84.108.75.223	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.214	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.243.31.2	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.210.186.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
213.57.183.33	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.55.154.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.94.45.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.121.96.233	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.228.212.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
216.243.31.2	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.243.31.2	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.154.81.78	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
84.109.74.20	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
213.8.204.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
188.161.112.11	Palestinian Territory Occupied	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.243.31.2	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-23-2016-19:04:05 to 09-23-2016-20:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.120.148.124	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	238
176.13.23.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
77.139.59.226	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/drushim/	Block	3
85.250.179.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.121.150.234	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
79.181.163.119	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/1/size338x0/1531.jpg	Block	2
77.139.59.226	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.59.226	Block	2
163.172.52.197	United Kingdom	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/admin/i18n/readme.txt	Block	1
207.46.13.110	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12535-he/dov	Block	1
84.108.15.169	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1474-he/refuah.aspx	Block	1
163.172.52.197	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/admin/i18n/readme.txt	Block	1
79.180.62.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.64.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
100.38.169.4	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.230.186	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
2.53.179.184	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
176.13.232.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.65.152	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
109.253.204.105	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/piwik.php	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2308.jpg	Block	1

09-23-2016-19:04:05 to 09-23-2016-20:04:05