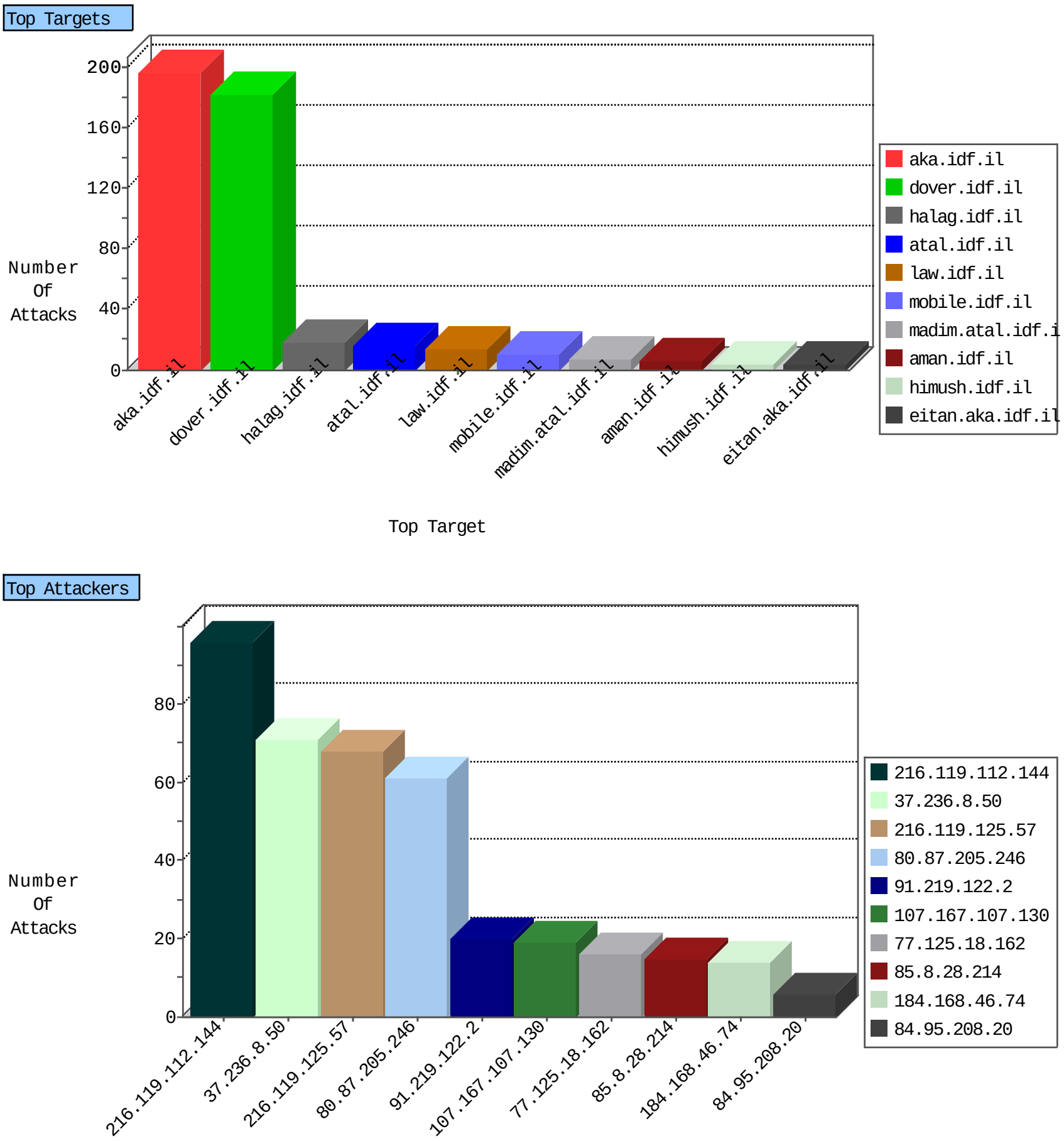
09-26-2016-05:04:06 to 09-26-2016-06:04:06

IDF Under Attack
Daily Report



09-26-2016-05:04:06 to 09-26-2016-06:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	1633
111.73.45.16	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
45.32.205.193	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
204.12.220.82	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
63.141.231.210	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
204.12.220.86	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1

09-26-2016-05:04:06 to 09-26-2016-06:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.119.112.144	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	18
85.8.28.214	Sweden	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	13
216.119.125.57	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
184.168.46.74	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.112.144	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.2	Poland	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.57	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
85.8.28.214	Sweden	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
95.135.249.88	Ukraine	147.237.77.216	dover.idf.il	12580: HTTP: SQL Injection (Cookie Header)	Block	1

09-26-2016-05:04:06 to 09-26-2016-06:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.119.112.144	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	72
216.119.125.57	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	51
91.219.122.2	147.237.72.166	Poland	aka.idf.il	SQL Injection - Select From	14
184.168.46.74	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
116.209.196.7	147.237.77.74	China	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
68.190.208.191	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 4096	1
68.190.208.191	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -f -sS	1
210.212.207.80	147.237.76.30	India	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.24.228.20	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
178.212.76.3	147.237.76.200	Russian Federation	eitan.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
118.71.70.197	147.237.0.15	Vietnam	kosher-kravi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.187.45.144	147.237.76.198	Japan	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN Potential SSH Scan	1
78.129.171.173	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN Potential SSH Scan	1
68.190.208.191	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 2048	1
46.161.40.17	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
201.7.217.249	147.237.77.212	Brazil	e.dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
183.106.209.187	147.237.8.24	Korea, Republic of	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
177.126.12.11	147.237.77.19	Brazil	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.129.171.173	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN Potential SSH Scan	1

09-26-2016-05:04:06 to 09-26-2016-06:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
37.236.8.50	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	64
107.167.107.130	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
77.125.18.162	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.50.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.236.8.50	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.236.8.50	Iraq	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.204	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.148.226	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
76.90.211.5	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
198.7.57.46	United States	147.237.0.19	madim.atal.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
2.53.133.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
187.61.109.18	Brazil	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
207.244.95.125	United States	147.237.77.243	mobile.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
184.105.139.120	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
2.55.188.208	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.50	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
80.87.205.246	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
189.74.210.150	Brazil	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
67.45.114.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.84	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
99.250.108.51	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.219	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.55.188.208	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.60	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.15	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.0.101.216	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.88	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
76.90.211.5	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
216.218.206.120	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.232	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
5.102.218.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.61	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
84.61.62.0	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.82.47.29	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.112	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
138.246.253.19	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.120.203.47	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.235	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.148.226	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.163	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
93.172.142.97	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.37	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
207.46.13.112	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.139.112	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.55.188.208	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.49	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-26-2016-05:04:06 to 09-26-2016-06:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
207.244.95.125	United States	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.53.50.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
198.7.57.46	United States	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1
198.7.57.46	United States	147.237.0.19	madim.atal.idf.i	Unauthorized Method HEAD for 147.237.0.19/	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/piwik.php	Block	1
37.236.8.50	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
207.46.13.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wepdwullte5odk5nji2ntmpzbyczg9kfgjmd2qwagidd2qwbaihdw8wah4hvmlzawjszwhkzaild2qwbaibd2qwagibdxychgrocmvmbqxkzwzhdwx0lmfzchhkagupzbycagepfgiebxn0ewxlbqt3awr0ado5ntbwebyeagepfgiecwlubmvyahrtbauz16nxknec15xxqidxldeq16nxlder15xxqmqcag8wah8cbqt3awr0ado5ntbwegqyaquex19db250cm9sc1jlcxvpcmvqb3n0qmfja0tlev9ffgmffmn0bdawjgn0bdawjhjivghpc1npdguffmn0bdawjgn0bdawjhjiqwxsu2l0zxmffmn0bdawjgn0bdawjhjiqwxsu2l0zxm8eh5yubarwrcttqtsdbjv4srbosmtntap+hah2uc8vg==	Block	1
104.173.227.88	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.120.203.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
207.46.13.180	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
77.125.18.162	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
192.116.176.221	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
66.249.64.147	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
207.244.95.125	United States	147.237.77.243	mobile.idf.il	Unauthorized Method HEAD for 147.237.77.243/	Block	1

09-26-2016-05:04:06 to 09-26-2016-06:04:06