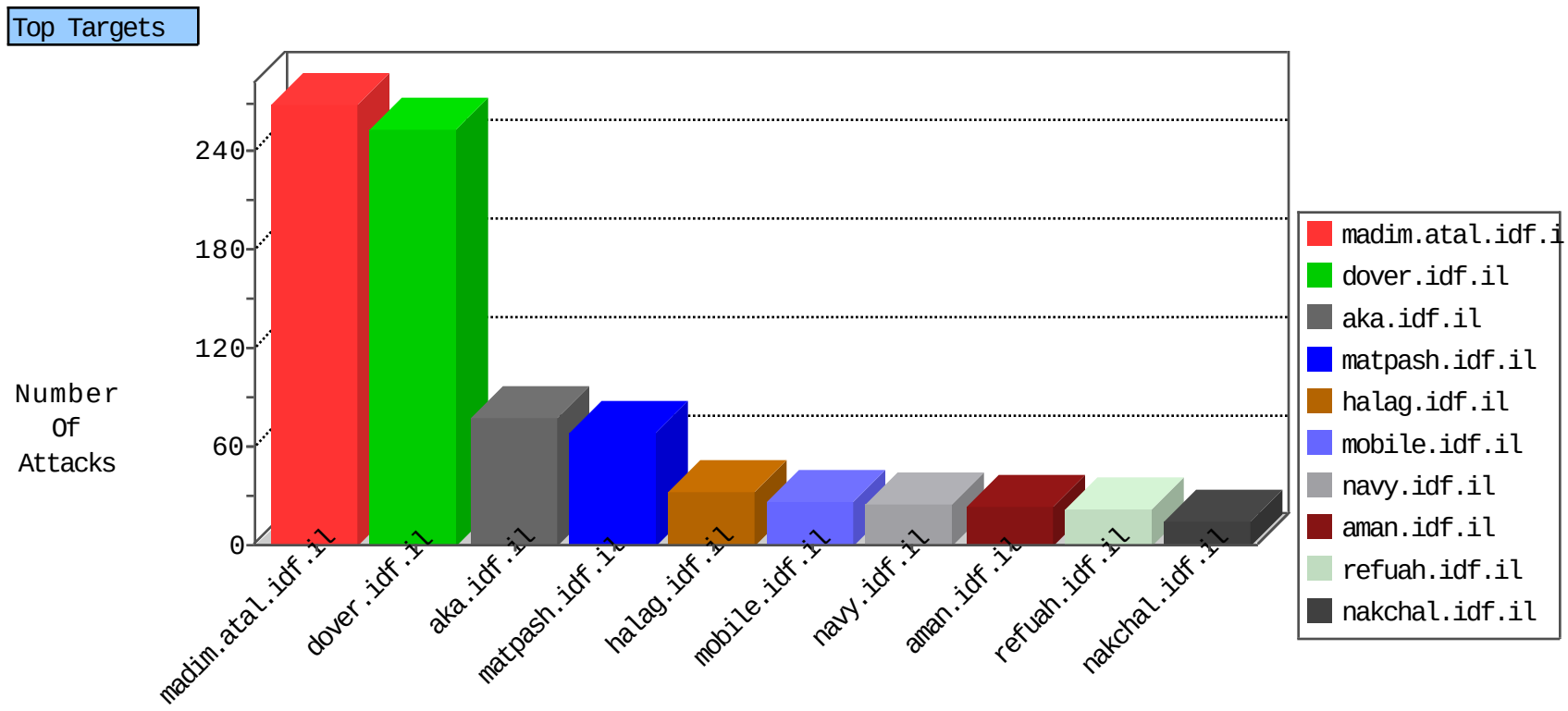
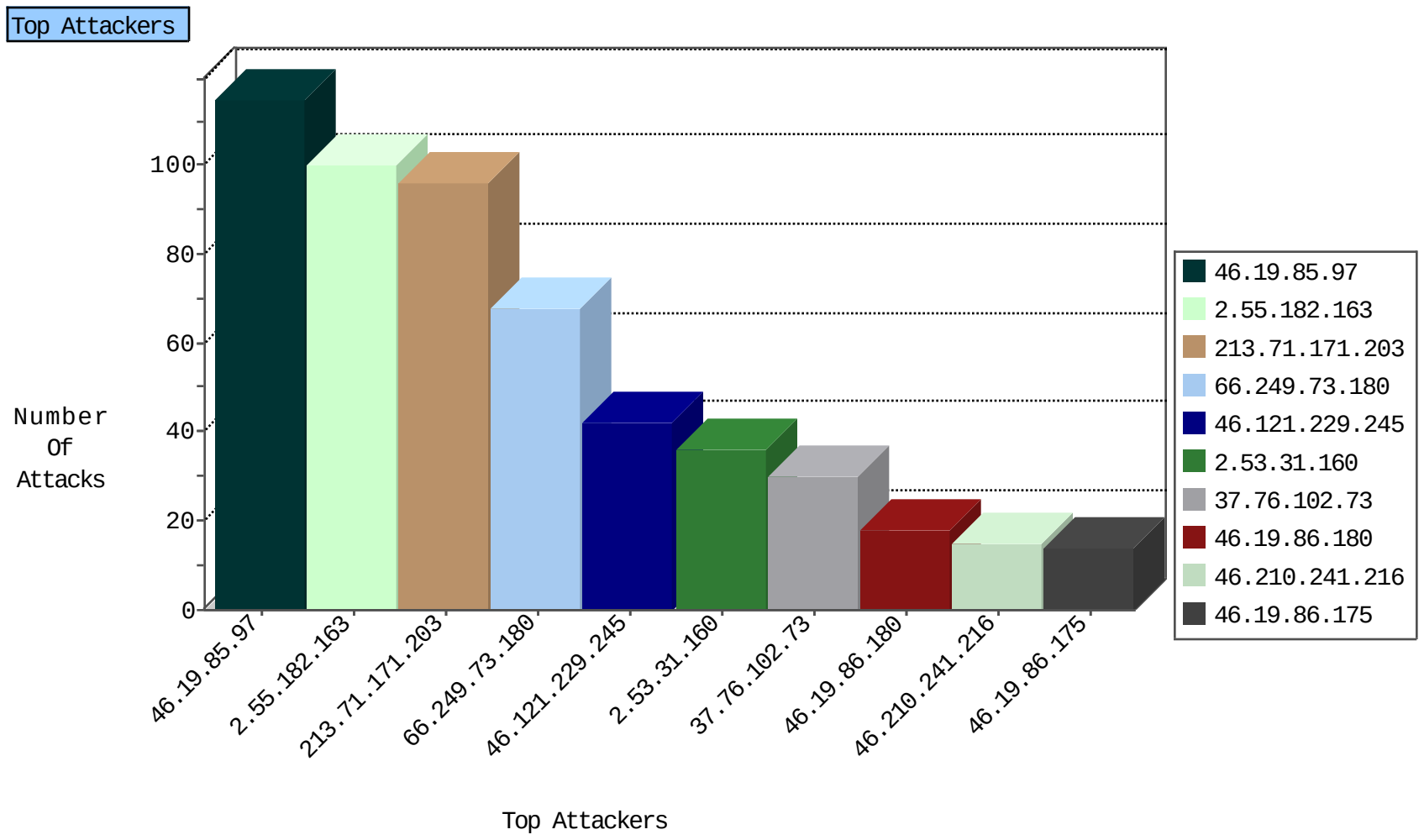
09-23-2016-17:04:01 to 09-23-2016-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-23-2016-17:04:01 to 09-23-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.76.109.178	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
141.212.122.118	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
223.17.126.192	Hong Kong	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
198.55.103.48	United States	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
198.55.103.48	United States	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	1

09-23-2016-17:04:01 to 09-23-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.234.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-23-2016-17:04:01 to 09-23-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.73.180	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	68
115.208.231.65	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
211.197.201.106	147.237.76.39	Korea, Republic of	mobile.meitav.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
190.83.139.178	147.237.0.200	Trinidad and Tobago	m4u.idf.il	ET SCAN NMAP -f -sS	1
163.172.129.15	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.187.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
113.72.177.138	147.237.77.19	China	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.73.163	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
46.183.223.228	147.237.8.46	Latvia	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
190.83.139.178	147.237.0.200	Trinidad and Tobago	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
180.213.5.205	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
2.55.130.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-23-2016-17:04:01 to 09-23-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.71.171.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
37.76.102.73	Hungary	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
46.210.241.216	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.76.102.73	Hungary	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	13
87.69.119.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.179	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.58.151	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.216	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.121.229.245	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.207.13	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.121.229.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.121.229.245	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.121.229.245	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.121.229.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.121.229.245	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.231.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.121.229.245	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.18	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.130.254.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.120.174.214	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
109.67.55.74	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.120.174.214	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
141.0.14.125	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.55.39.187	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
84.109.44.236	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.116.218.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
79.182.31.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.218.13	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.85.211	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.85.83	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.121.229.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
85.130.254.85	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
31.154.49.33	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
2.55.141.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.45	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.2.238	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.148.254	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.129.69	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.39.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.121.229.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
176.13.8.163	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2

09-23-2016-17:04:01 to 09-23-2016-18:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
2.55.182.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
2.53.31.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
176.13.9.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
218.87.49.237	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 218.87.49.237	Block	3
84.229.9.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	2
2.53.150.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.153.236	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.3.44	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
66.249.93.85	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
66.249.76.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/aman	Block	1
46.19.85.72	Israel	147.237.76.42	refuah.idf.il	Abnormally Long Request request version	Block	1
2.55.50.131	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
82.80.130.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
176.13.11.114	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.85.18	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
67.53.18.178	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
46.19.85.72	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version _pk_ref.118.fd1c=%5B%22%22%2C%22%22%2C1474642682%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D; _pk_id.118.fd1c=f50bc727e1df93dd.1472629351.3.1474642682.1474642682.; _pk_ses.118.fd1c=*	Block	1
218.87.49.237	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
46.117.153.226	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
195.78.246.252	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus	Block	1
46.19.85.18	Israel	147.237.76.31	nakchal.idf.il	Multiple Malformed URL from 46.19.85.18	Block	1
2.53.58.151	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.231.57	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/e.navy.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.70	Block	1
46.19.85.72	Israel	147.237.76.42	refuah.idf.il	Malformed URL __atuvs=57e542f751da6a47000;	Block	1
109.64.89.65	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.76.102.73	Hungary	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
66.249.66.197	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-22724-he/idfgdover.aspx	Block	1
204.79.180.6	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
46.19.85.18	Israel	147.237.76.31	nakchal.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.18	Block	1
77.138.121.80	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.76.70	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/apple-app-site-association	Block	1
46.19.85.72	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method %2C1%7C38; in URL __atuvs=57e542f751da6a47000	Block	1
109.65.71.253	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
37.142.187.59	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17380-he/dover.aspx	Block	1
66.249.76.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.57	Block	1
46.19.85.18	Israel	147.237.76.31	nakchal.idf.il	Unknown HTTP Request Method 3d in URL	Block	1
217.132.137.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
79.177.196.216	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.19.85.18	Israel	147.237.76.31	nakchal.idf.il	Illegal HTTP Version	Block	1

09-23-2016-17:04:01 to 09-23-2016-18:04:01