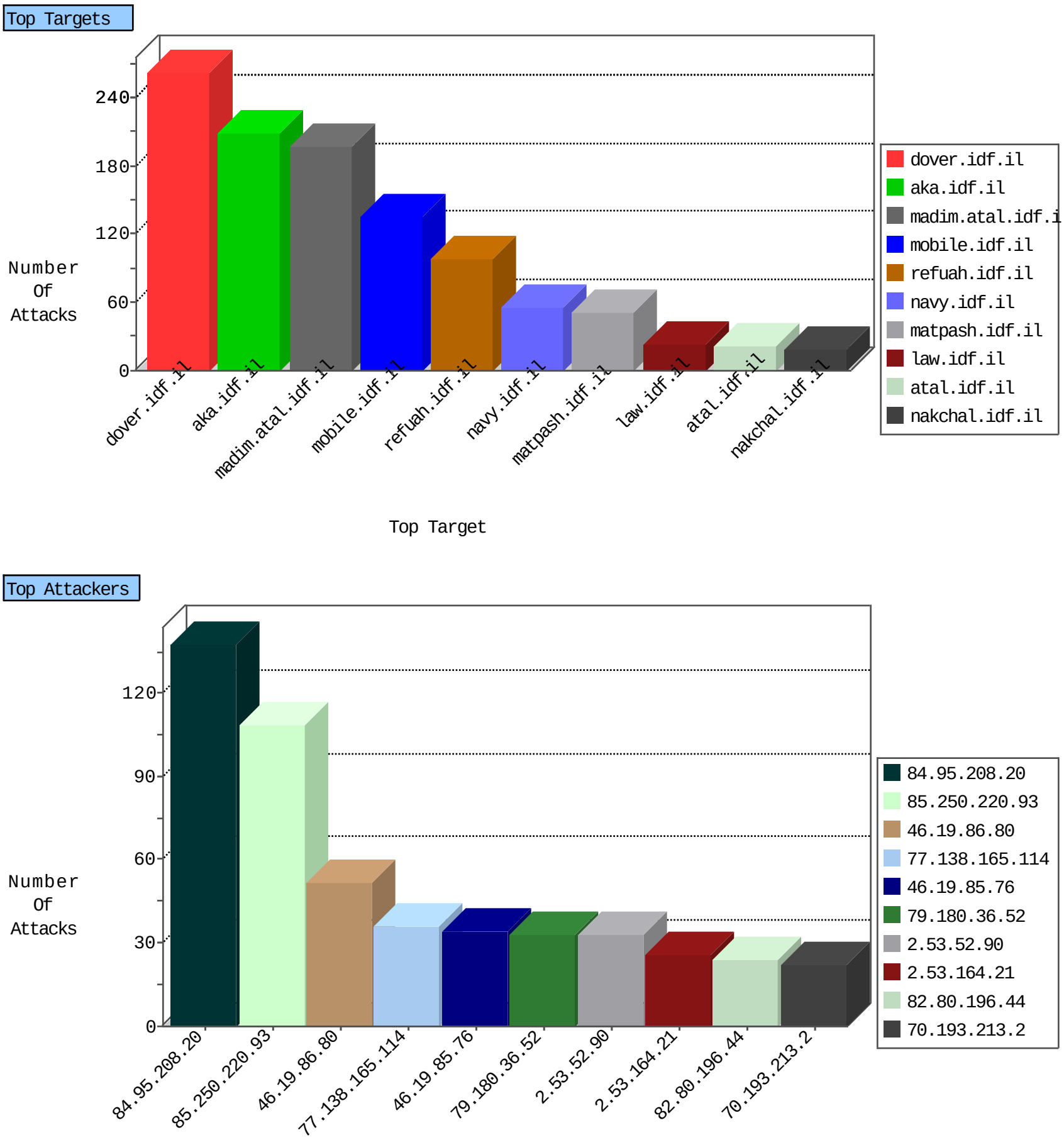
09-01-2016-11:04:03 to 09-01-2016-12:04:03

IDF Under Attack Daily Report



09-01-2016-11:04:03 to 09-01-2016-12:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
190.82.85.70	Chile	147.237.76.86	navy.idf.il	L4 Source or Dest Port Zero	drop	3
5.189.186.243	Germany	147.237.76.201	e.atal.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.197	e.himush.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.202	e.halag.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
46.19.86.123	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.189.186.243	Germany	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1
5.189.186.243	Germany	147.237.76.196	e.sviva.idf.il	Black List	drop	1

09-01-2016-11:04:03 to 09-01-2016-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.9.70.189	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	4
176.9.70.189	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	4
162.210.196.130	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-01-2016-11:04:03 to 09-01-2016-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.229.59.228	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	6
84.229.59.228	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	6
192.115.215.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.172	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
147.236.38.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.215.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.17.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
23.82.46.210	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.222.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.198.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.6.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.23.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.225.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.139.188.87	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
188.120.135.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.41.77	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
146.200.12.249	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
23.82.46.210	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.77.227	Turkey	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.7.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.28.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.62.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.92.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.129.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

09-01-2016-11:04:03 to 09-01-2016-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.180.36.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
2.53.52.90	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	24
213.42.197.201	United Arab Emirates	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	20
141.226.217.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
74.208.230.195	United States	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	17
46.19.86.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.86.80	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
2.53.142.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.86.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
212.150.37.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
176.228.215.236	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
46.18.21.235	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.133	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.53.135.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
176.13.237.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
70.193.213.2	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.165	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.253.128.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.228.215.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
89.139.151.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.253.214.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.135.100	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
74.208.218.66	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
70.193.213.2	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
46.19.86.85	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.244	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
70.193.213.2	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
185.32.179.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.10	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.10	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.36	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.244	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.178.123.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
138.246.253.19	Germany	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
138.246.253.19	Germany	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.19.85.213	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.231.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.18.21.235	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
82.102.168.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
81.28.51.108	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-01-2016-11:04:03 to 09-01-2016-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.220.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	109
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	79
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	36
46.19.85.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
2.53.164.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
77.138.165.114	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	25
113.97.235.62	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 113.97.235.62	Block	15
77.138.165.114	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.138.165.114	Block	11
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	9
2.53.52.90	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
113.97.235.62	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6
79.180.36.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
46.210.187.45	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.55.139.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.219.174.67	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	3
2.55.157.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.214.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
62.219.174.67	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	3
62.219.174.67	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.55.139.58	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
46.19.85.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.142.42	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.68	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
87.69.222.244	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/images/	Block	2
212.179.22.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.22.6	Block	2
2.53.35.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.214.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
212.179.22.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/home/	Block	1
77.139.39.200	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.39.200	Block	1
176.13.237.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/ שקופית5	Block	1
84.108.164.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mainasachar	Block	1
82.81.137.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
185.159.36.12		147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
128.177.161.142	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/giyus/	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.66.48.102	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 127.0.0.1/callback.json	Block	1
212.179.61.123	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
77.139.39.200	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/sachar	Block	1
180.76.15.10	China	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
66.249.83.45	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
46.210.187.45	Israel	147.237.0.19	madim.atal.idf.i	Double URL Encoding - parameter: ReturnUrl in madim.atal.idf.il/mobile/login.aspx	Block	1
185.159.36.12		147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/hnap1/	Block	1
82.166.180.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.226.217.98	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.69.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/ שקופית4	Block	1
109.253.128.160	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
212.179.61.123	Israel	147.237.76.86	navy.idf.il	Multiple Abnormally Long Request from 212.179.61.123	Block	1

09-01-2016-11:04:03 to 09-01-2016-12:04:03