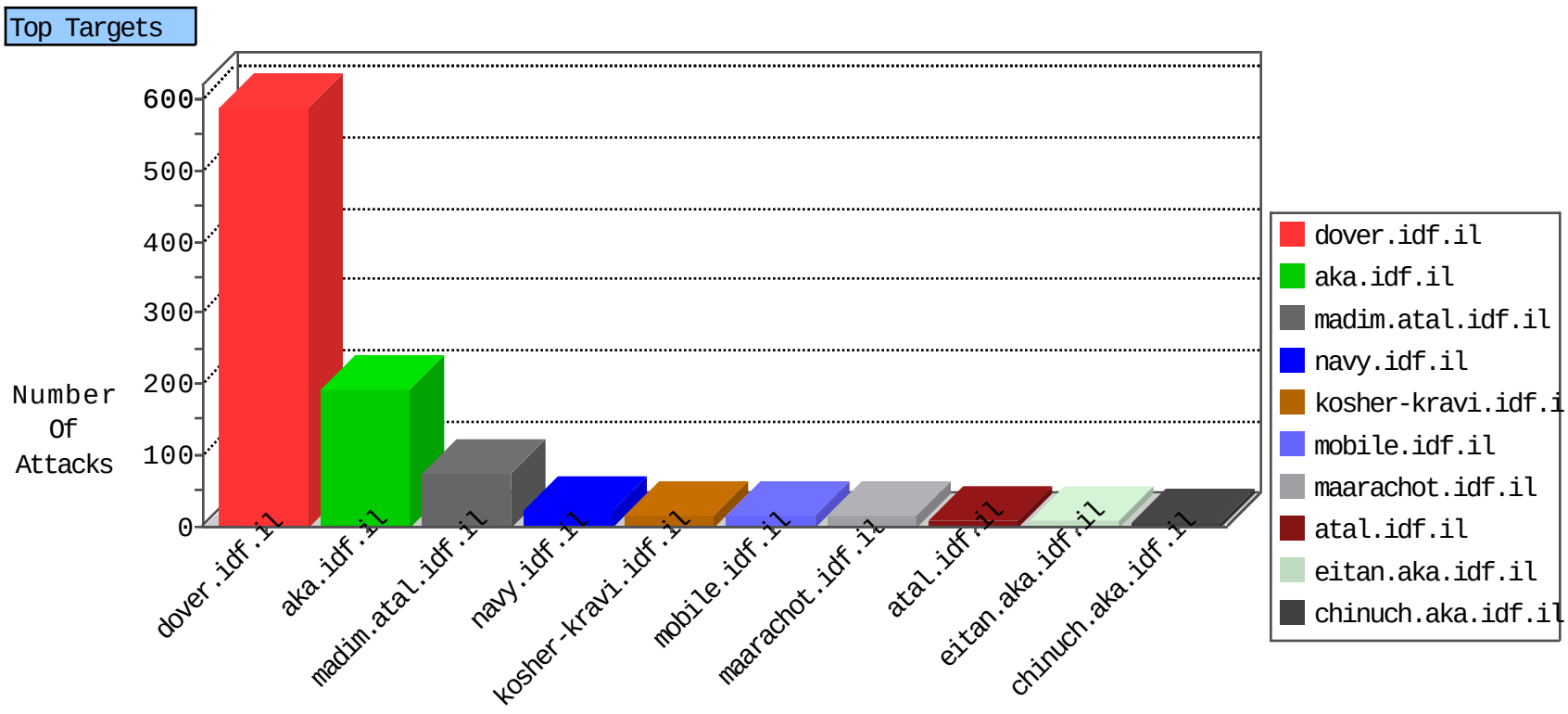
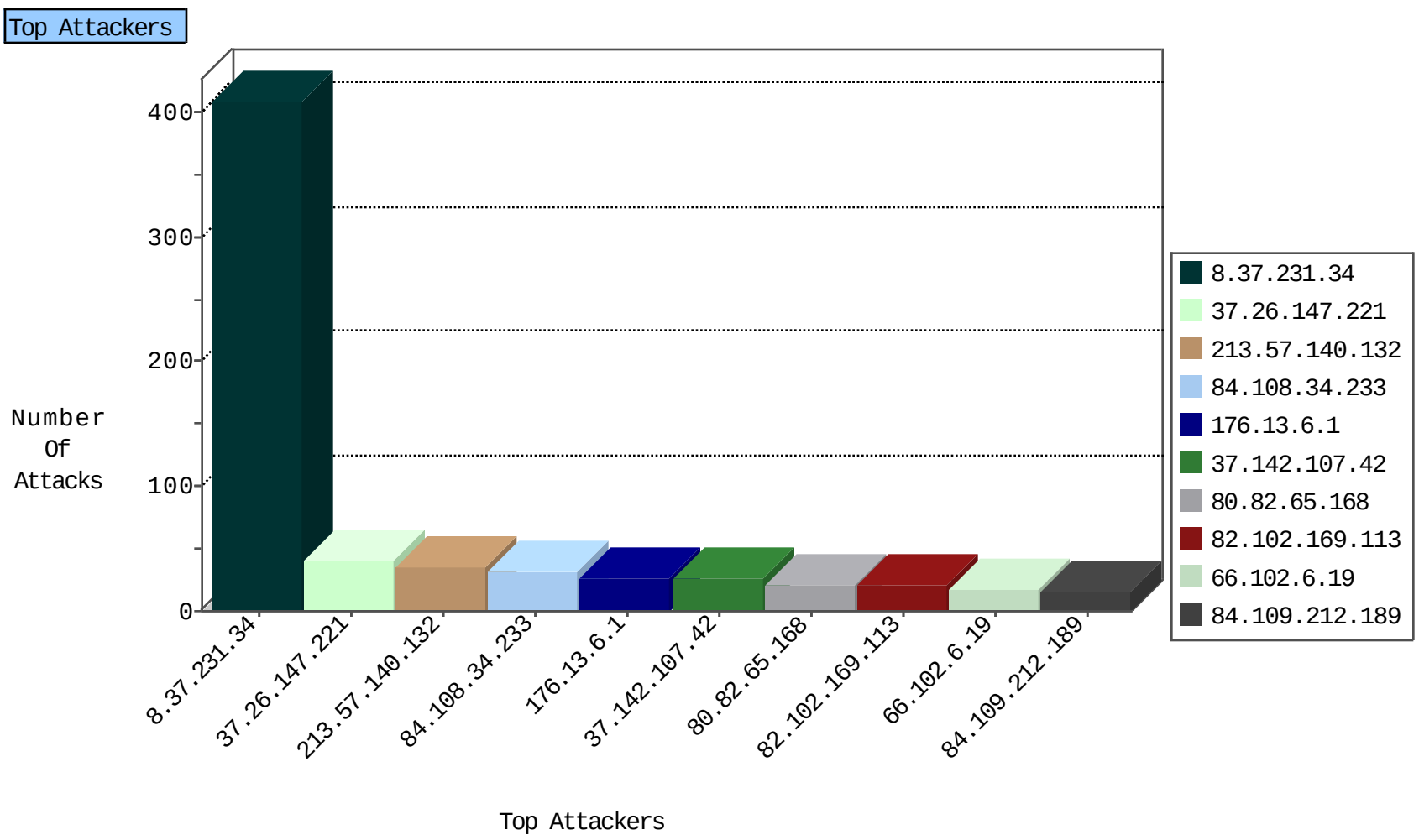
09-30-2016-07:04:05 to 09-30-2016-08:04:05

IDF Under Attack Daily Report





09-30-2016-07:04:05 to 09-30-2016-08:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.140.132	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
66.102.6.19	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
8.37.231.34	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	5
217.132.40.32	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
66.102.6.17	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
66.102.6.21	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.231.34	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
173.252.123.134	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
80.246.130.139	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
188.219.39.3	Italy	147.237.76.147	chinuch.aka.idf.il	L4 Source or Dest Port Zero	drop	2
204.42.253.2	United States	147.237.76.86	navy.idf.il	Black List	drop	2
89.248.172.173	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
8.37.231.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-30-2016-07:04:05 to 09-30-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.82.65.168	Netherlands	147.237.0.15	kosher-kravi.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	10
208.110.85.74	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	5
80.82.65.168	Netherlands	147.237.0.19	madim.atal.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
208.110.85.74	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
80.82.65.168	Netherlands	147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	2
208.110.85.74	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	2
208.110.85.74	United States	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
80.82.65.168	Netherlands	147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

09-30-2016-07:04:05 to 09-30-2016-08:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	14
80.82.65.168	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	2
78.129.171.173	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
183.129.160.229	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.65.168	147.237.0.19	Netherlands	madim.atal.idf.il	ET WEB_SERVER Muieblackcat scanner	1
78.129.171.173	147.237.77.74	United Kingdom	law.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.109	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
211.149.222.5	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
92.29.69.152	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1

09-30-2016-07:04:05 to 09-30-2016-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	313
8.37.231.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	73
84.108.34.233	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
84.108.34.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
8.37.231.34	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
176.13.6.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
2.53.136.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
213.57.140.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
5.29.118.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
62.0.225.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
110.92.99.2	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.65.44	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.102.6.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
77.126.50.189	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.142.107.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
176.13.6.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
2.55.27.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.26.59	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.140.132	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
37.142.107.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.14.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.147.221	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence		alert	4
66.102.6.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.142.107.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
82.102.169.113	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.221	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence		monitor	4
37.142.107.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.102.6.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.142.107.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
109.65.61.58	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
77.127.51.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.239.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.201	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.243.55.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
37.26.147.221	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.127.132	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.130.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.75	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.142.107.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.6.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
176.13.235.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.6.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.86.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

09-30-2016-07:04:05 to 09-30-2016-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
84.109.212.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
37.26.147.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
77.139.9.156	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	4
213.57.132.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
95.86.110.70	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 95.86.110.70	Block	2
157.55.39.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.79.169	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
5.29.238.87	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
176.13.16.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
46.19.86.208	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
216.4.56.161	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
66.249.69.236	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1682	Block	1
176.13.233.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/7	Block	1
72.131.28.44	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
46.19.86.208	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 220.181.125.23	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1314-he/refuah.aspx	Block	1
192.243.55.132	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/tmuna	Block	1
77.138.7.85	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar	Block	1
46.19.86.208	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_ses.20.8afc=*	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1413-he/atal.aspx	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
40.77.167.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/gallery	Block	1
46.19.86.208	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method 50c015173980.1471982072.5.1475208748.1475208748.; in URL _pk_ses.20.8afc=*	Block	1

09-30-2016-07:04:05 to 09-30-2016-08:04:05