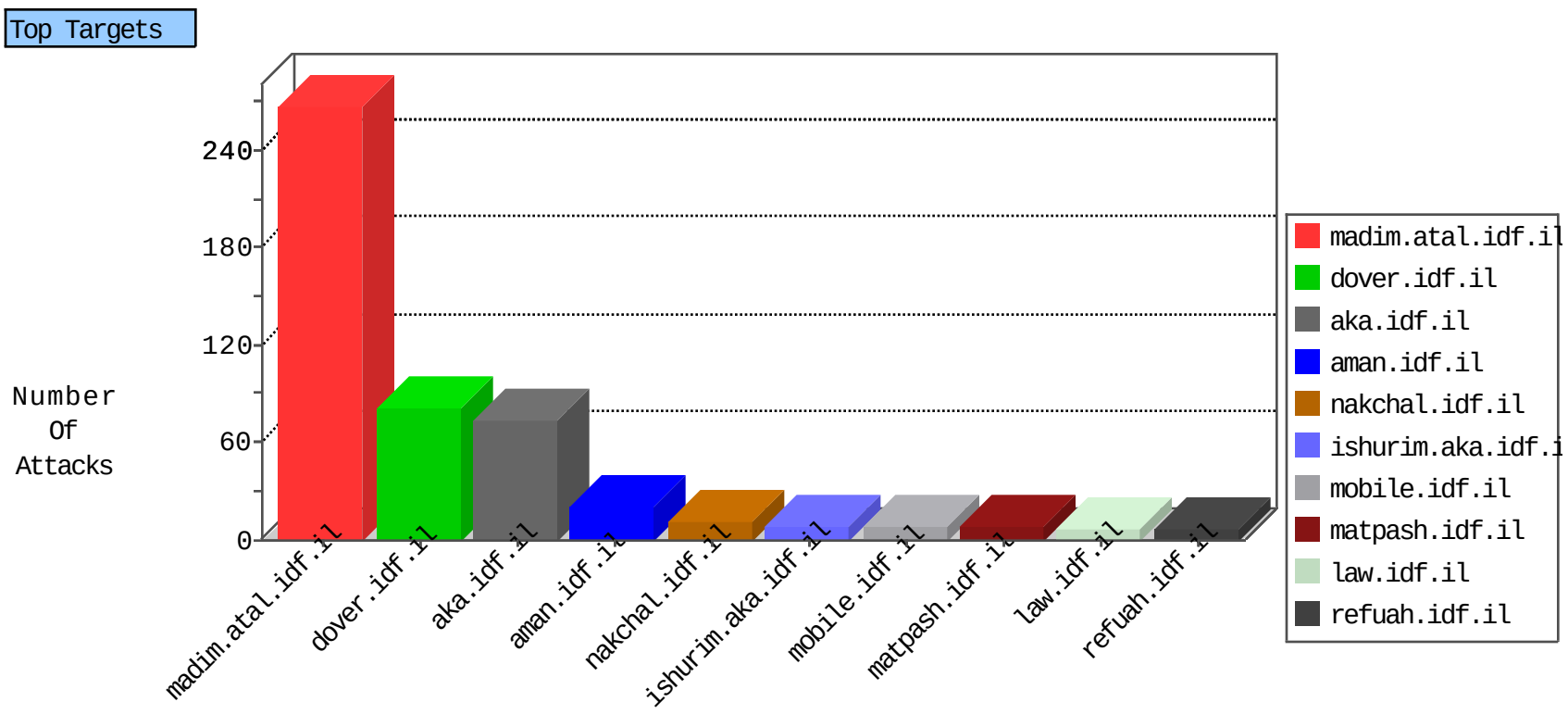
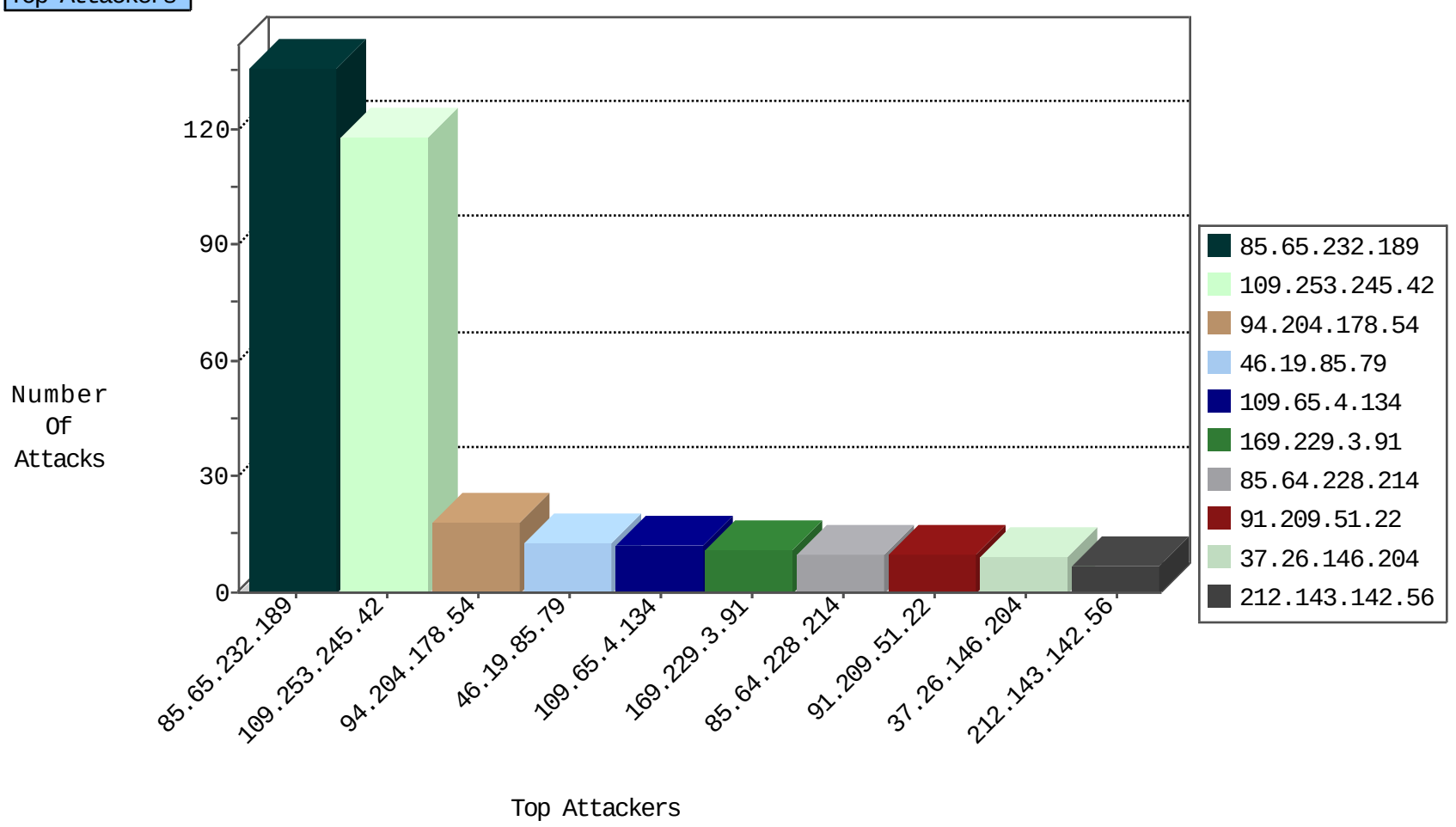
09-26-2016-00:04:00 to 09-26-2016-01:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-26-2016-00:04:00 to 09-26-2016-01:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
163.172.67.79	United Kingdom	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
163.172.67.79	United Kingdom	147.237.76.42	refuah.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
163.172.67.79	United Kingdom	147.237.76.44	e.refuah.idf.il	Black List	drop	1
114.4.66.96	Indonesia	147.237.77.235	sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

09-26-2016-00:04:00 to 09-26-2016-01:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.209.51.22	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	7
91.209.51.22	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
69.30.198.202	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-26-2016-00:04:00 to 09-26-2016-01:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
114.4.66.96	147.237.76.30	Indonesia	himush.idf.il	ET SCAN Potential SSH Scan	1
111.132.74.212	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 3072	1
189.161.104.96	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
46.183.223.228	147.237.77.121	Latvia	e.navy.idf.il	ET SCAN Potential SSH Scan	1
185.129.148.230	147.237.76.34	Latvia	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.28.189	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
124.8.223.198	147.237.76.86	Taiwan	navy.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.0.16	Taiwan	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
114.4.66.96	147.237.76.34	Indonesia	yohalan.idf.il	ET SCAN Potential SSH Scan	1
114.4.66.96	147.237.72.166	Indonesia	aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
189.161.104.96	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
46.183.223.228	147.237.76.44	Latvia	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
171.232.8.24	147.237.8.45	Vietnam	e.eitan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.63.28.189	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
124.8.223.198	147.237.76.199	Taiwan	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
124.8.223.198	147.237.0.19	Taiwan	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
114.4.66.96	147.237.76.38	Indonesia	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

09-26-2016-00:04:00 to 09-26-2016-01:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.204.178.54	United Arab Emirates	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.65.4.134	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
85.64.228.214	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
37.26.146.204	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.66.164.12	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.242.217	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.53.13.116	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
188.247.78.89	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
95.86.90.192	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.210.186.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
93.47.226.103	Italy	147.237.77.216	dover.idf.il	SYN Attack		monitor	3
79.181.137.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	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
64.134.54.125	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.145	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
109.253.245.42	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
188.120.154.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.253.193.224	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
37.26.147.176	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.25	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.129.86	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.197	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
185.3.147.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.147.200	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.142.33	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
197.235.183.2	Mozambique	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
99.99.226.117	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
151.80.44.115	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
109.253.150.54	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
188.120.154.79	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.134.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.8.24	e.lifestyle.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.162	United States	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
195.60.235.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.253.192.249	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
176.13.2.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
95.35.60.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
80.82.24.129	Poland	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.173	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.247.84.214	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1

09-26-2016-00:04:00 to 09-26-2016-01:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.65.232.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
109.253.245.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
85.64.212.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.193.224	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	4
185.32.179.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
83.130.66.16	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.17	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.179	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1117-7770-he/nakhal.aspx	Block	1
207.46.13.180	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
109.65.64.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
87.71.243.222	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
213.8.204.1	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
84.108.87.238	Israel	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
95.35.60.190	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on www.chamatz.aka.idf.il/404.aspx	Block	1
77.138.86.176	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
213.8.204.1	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
84.108.87.238	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
64.134.54.125	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
107.184.23.84	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 107.184.23.84	Block	1
77.139.175.83	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1
213.8.204.17	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
159.122.133.243	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to main/home/default.aspx	Block	1
66.249.64.157	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
107.184.23.84	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
81.223.254.34	Austria	147.237.77.234	halag.idf.il	Unauthorized URL Access to /robots.txt	Block	1

09-26-2016-00:04:00 to 09-26-2016-01:04:00