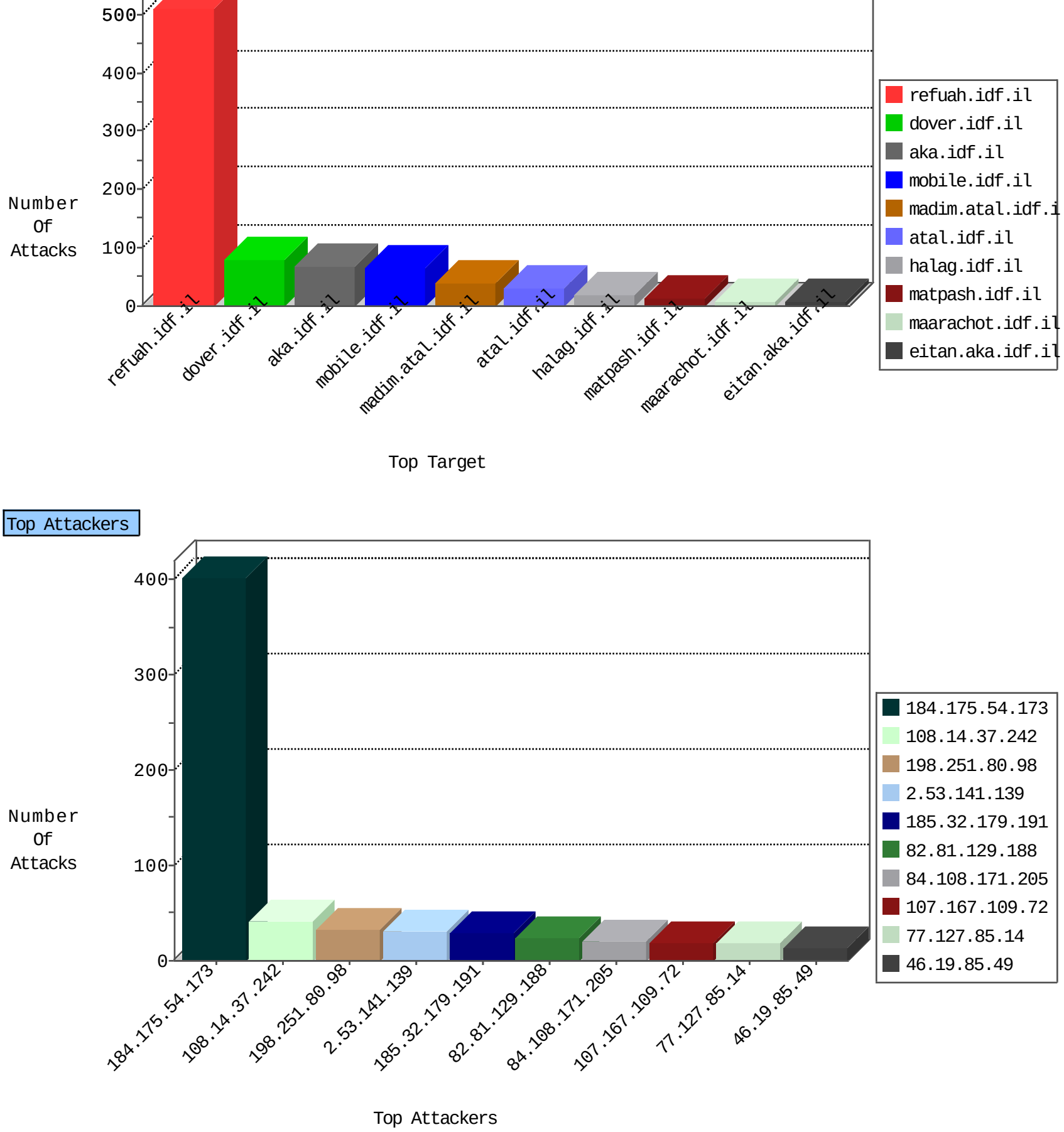
10-02-2016-00:04:04 to 10-02-2016-01:04:04

IDF Under Attack Daily Report



10-02-2016-00:04:04 to 10-02-2016-01:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
54.208.171.33	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.248.172.16	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1

10-02-2016-00:04:04 to 10-02-2016-01:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	5
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
106.38.241.106	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	3

10-02-2016-00:04:04 to 10-02-2016-01:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.29.140	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
201.38.68.132	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.72.217	United Kingdom	e.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.170.66	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.210.243.100	147.237.72.156	France	aman.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
52.187.42.85	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
94.102.48.194	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.13	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1

10-02-2016-00:04:04 to 10-02-2016-01:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
184.175.54.173	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	402
2.53.141.139	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
82.81.129.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
107.167.109.72	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
77.127.85.14	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
84.108.171.205	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
108.14.37.242	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
108.14.37.242	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
108.14.37.242	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	10
198.251.80.98	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	8
108.14.37.242	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
198.251.80.98	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
185.118.140.205	Turkey	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
198.251.80.98	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
93.172.159.143	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
198.251.80.98	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	7
46.19.85.49	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.171	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
129.171.6.40	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.92.23.98		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
198.251.80.98	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
37.26.148.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
2.55.39.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
108.14.37.242	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.49	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.53.63.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
92.222.245.134	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
92.222.245.134	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.22.134.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.13.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
5.60.220.192	Poland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
85.130.232.63	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.144.216	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
176.13.17.42	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
85.130.232.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
154.97.55.31	Sudan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
77.127.57.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.49	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
92.222.245.134	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
31.44.131.70	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.130.232.63	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
154.97.55.31	Sudan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.22.134.69	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
84.229.66.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
172.56.13.0	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
31.168.144.157	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

10-02-2016-00:04:04 to 10-02-2016-01:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
80.246.136.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.32.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
64.20.10.221	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	3
2.55.133.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	2
77.138.237.127	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
217.132.73.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
201.214.111.14	Chile	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
31.44.131.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	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
80.246.137.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
204.79.180.242	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
77.138.253.93	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers	Block	1
46.19.85.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1074-he/atal.aspx	Block	1
84.108.171.205	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1781-he/dover.aspx	Block	1
209.148.36.35	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
77.139.69.182	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk/	Block	1
46.116.85.172	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
91.246.101.53	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
77.138.82.43	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
213.151.45.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/m/ain/givus	Block	1
79.181.100.57	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.138.147.39	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash2017/lobby.aspx	Block	1

10-02-2016-00:04:04 to 10-02-2016-01:04:04