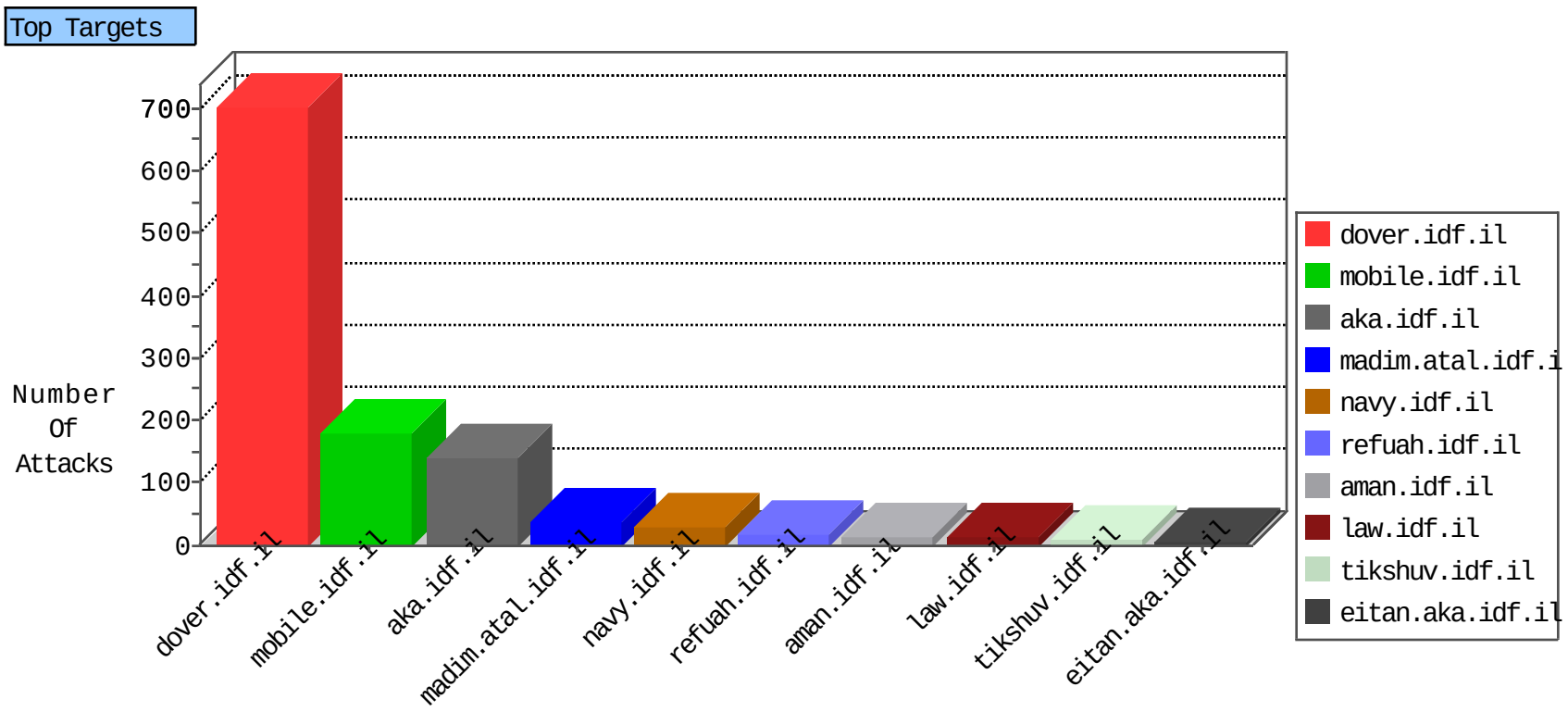
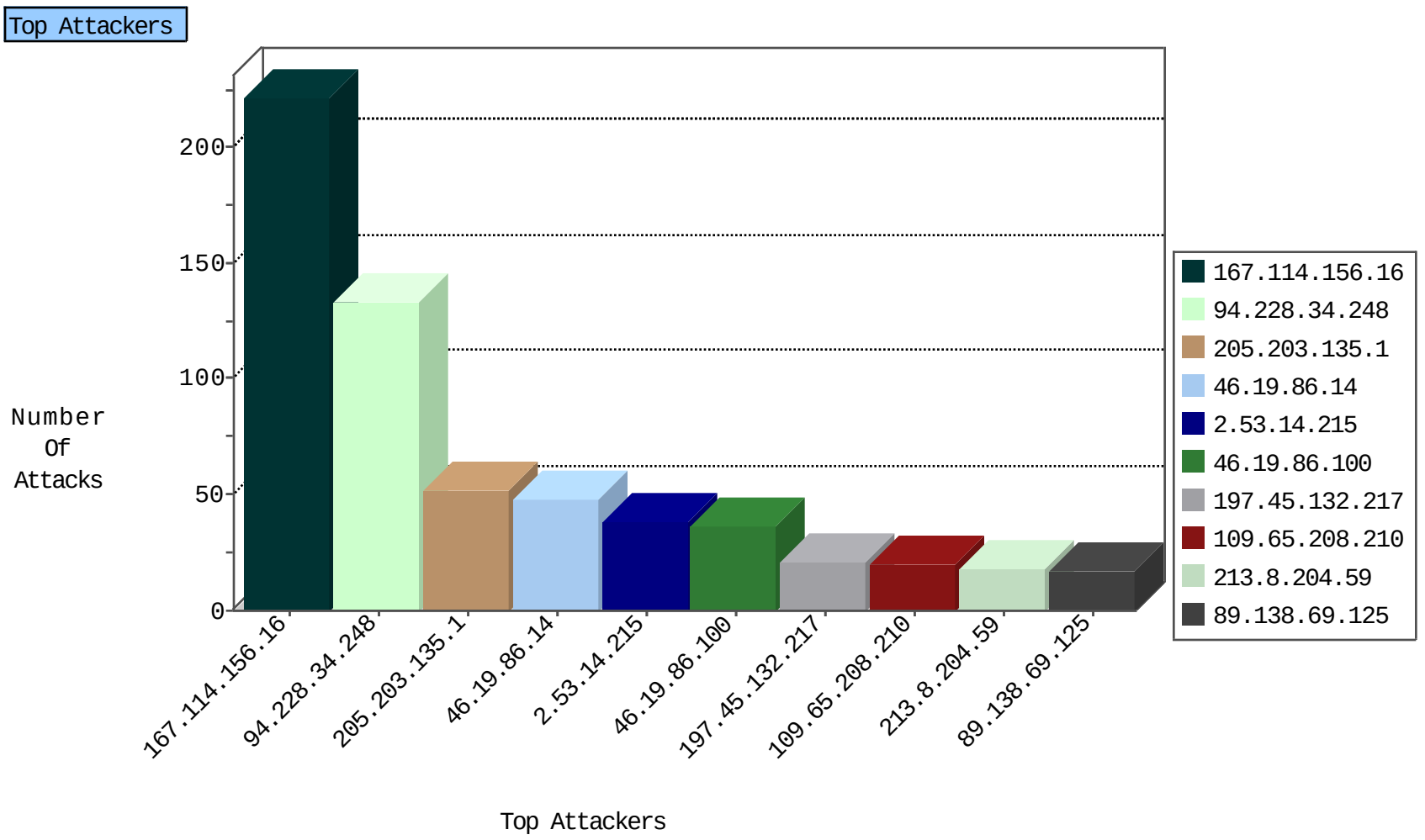
05-01-2016-01:04:05 to 05-01-2016-02:04:05

IDF Under Attack
Daily Report

Top Targets



Top Attackers



05-01-2016-01:04:05 to 05-01-2016-02:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	8660
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	313
212.143.254.66	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	7
79.179.15.37	Israel	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	3
82.221.105.7	Iceland	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
185.94.111.1	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

05-01-2016-01:04:05 to 05-01-2016-02:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-01-2016-01:04:05 to 05-01-2016-02:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
175.184.203.44	147.237.76.86	Australia	navy.idf.il	ET SCAN NMAP -sS window 3072	1
130.211.77.81	147.237.77.205	United States	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.204.211	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
37.26.148.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.56.4.53	147.237.77.216	Switzerland	dover.idf.il	portscan: TCP Distributed Portscan	1
175.184.203.44	147.237.76.86	Australia	navy.idf.il	ET SCAN NMAP -sS window 4096	1
130.211.77.81	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
130.211.77.81	147.237.76.44	United States	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.218.204.211	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
176.122.49.3	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

05-01-2016-01:04:05 to 05-01-2016-02:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	133
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
46.19.86.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
2.53.14.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
89.138.69.125	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.85.49	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.246.136.119	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.120.125.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
128.242.249.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.180.173.209	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
82.69.103.167	United Kingdom	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
130.203.136.75	United States	147.237.77.74	law.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	8
79.176.37.119	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.173.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
109.64.246.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.155.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.178.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.12	United States	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.132.228.45	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
67.248.53.208	United States	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.22.134.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.69.205.17	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.57.221.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
95.86.118.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
54.190.181.69	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.183.224.139	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.196.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.138.123.168	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

05-01-2016-01:04:05 to 05-01-2016-02:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.208.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
213.8.204.59	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.8.204.59	Block	17
46.19.86.100	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
2.53.14.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	8
81.218.241.26	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	6
5.144.60.236	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 5.144.60.236	Block	6
46.19.85.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.151.35.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.136.119	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
93.172.36.204	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
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
185.54.162.11	Netherlands	147.237.76.42	refuah.idf.il	Parameter Type Violation &l in www.refua.atal.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
51.255.65.5	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19072-he/dover.aspx	Block	1
5.144.60.236	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	1
213.8.204.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/[object object]	Block	1
95.86.118.223	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.176.37.119	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 106 cookies	Block	1
185.54.162.11	Netherlands	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/templates/sendtofriend/sendtofriend.aspx parameter &l	Block	1
81.218.241.26	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/2/size338x0/1652.jpg	Block	1
66.249.78.22	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
17.142.155.148	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
79.181.178.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.47.171	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
207.46.13.178	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
31.178.144.59	Poland	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
157.55.39.53	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18907-en/dover.aspx <a href=	Block	1
46.19.86.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.241.237.225	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3208.pdf	Block	1
176.13.4.187	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
50.153.245.38	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/894-he/eitan.aspx	None	1
5.144.60.236	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1

05-01-2016-01:04:05 to 05-01-2016-02:04:05