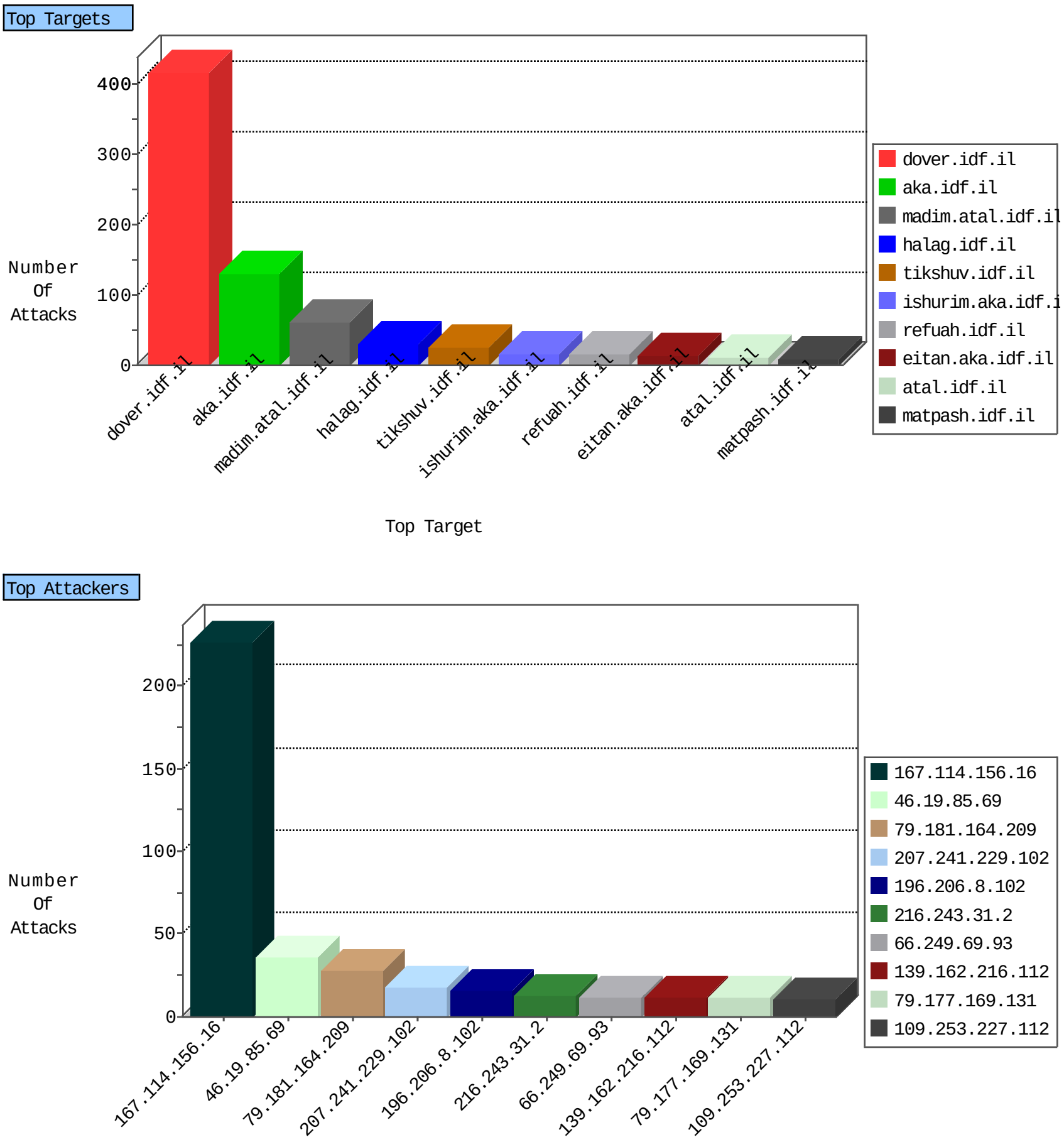
04-20-2016-21:04:01 to 04-20-2016-22:04:01

IDF Under Attack Daily Report



04-20-2016-21:04:01 to 04-20-2016-22:04:01

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	19834
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5718
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	3286
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	73
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
69.30.198.149	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
79.109.158.47	Spain	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
172.82.174.53	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
74.91.18.43	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
204.12.196.234	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
69.30.226.218	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
173.208.197.250	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
74.91.17.178	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
173.208.197.252	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
107.150.32.62	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
69.30.198.149	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
74.91.18.42	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
173.208.197.253	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1

04-20-2016-21:04:01 to 04-20-2016-22:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-20-2016-21:04:01 to 04-20-2016-22:04:01

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	5
37.26.149.148	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	2
109.57.96.106	147.237.77.216	Denmark	dover.idf.il	Xenu Link Sleuth User Agent	2
66.249.78.159	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
104.130.70.221	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.148.3	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
178.17.42.103	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
122.3.115.155	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.214.149.209	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
93.174.95.124	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.148.3	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
115.29.197.215	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
107.158.255.194	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

04-20-2016-21:04:01 to 04-20-2016-22:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.164.209	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
207.241.229.102	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
196.206.8.102	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.177.169.131	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.69.93	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.133.77	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
40.77.167.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
50.198.75.25	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
72.167.232.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.7.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.5	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.146.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.227.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.64.108.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.16.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.80.118	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.67.103.56	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.227.97	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.85.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.179.66.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.161.12.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.4.21	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
49.228.87.201	Thailand	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
93.158.152.201	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.254.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.227.112	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
176.13.3.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.114.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.66.14	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.216.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.16.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-20-2016-21:04:01 to 04-20-2016-22:04:01

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.27.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.100	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

04-20-2016-21:04:01 to 04-20-2016-22:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
185.32.179.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
176.13.7.16	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
176.232.94.167	Turkey	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
80.3.125.157	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.17	Block	1
173.208.197.250	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
80.246.133.77	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/960.css	Block	1
66.249.75.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
31.168.205.89	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
173.208.197.253	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.app-softwares.com/	Block	1
68.180.230.108	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	Block	1
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Friend.aspx?&l=he&f=1133&d=20978 in URL	Block	1
201.235.131.135	Argentina	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
85.65.25.145	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
37.26.149.148	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/megurim/home/default.asp	Block	1
69.30.198.149	United States	147.237.76.200	eitan.aka.idf.il	Distributed Unauthorized URL Access on www.app-softwares.com/	Block	1
46.121.67.215	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11043-en/dover	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
176.232.94.167	Turkey	147.237.77.74	law.idf.il	PHP Attempt	Block	1
79.181.164.209	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
54.229.19.112	Ireland	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
149.78.92.11	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1

04-20-2016-21:04:01 to 04-20-2016-22:04:01