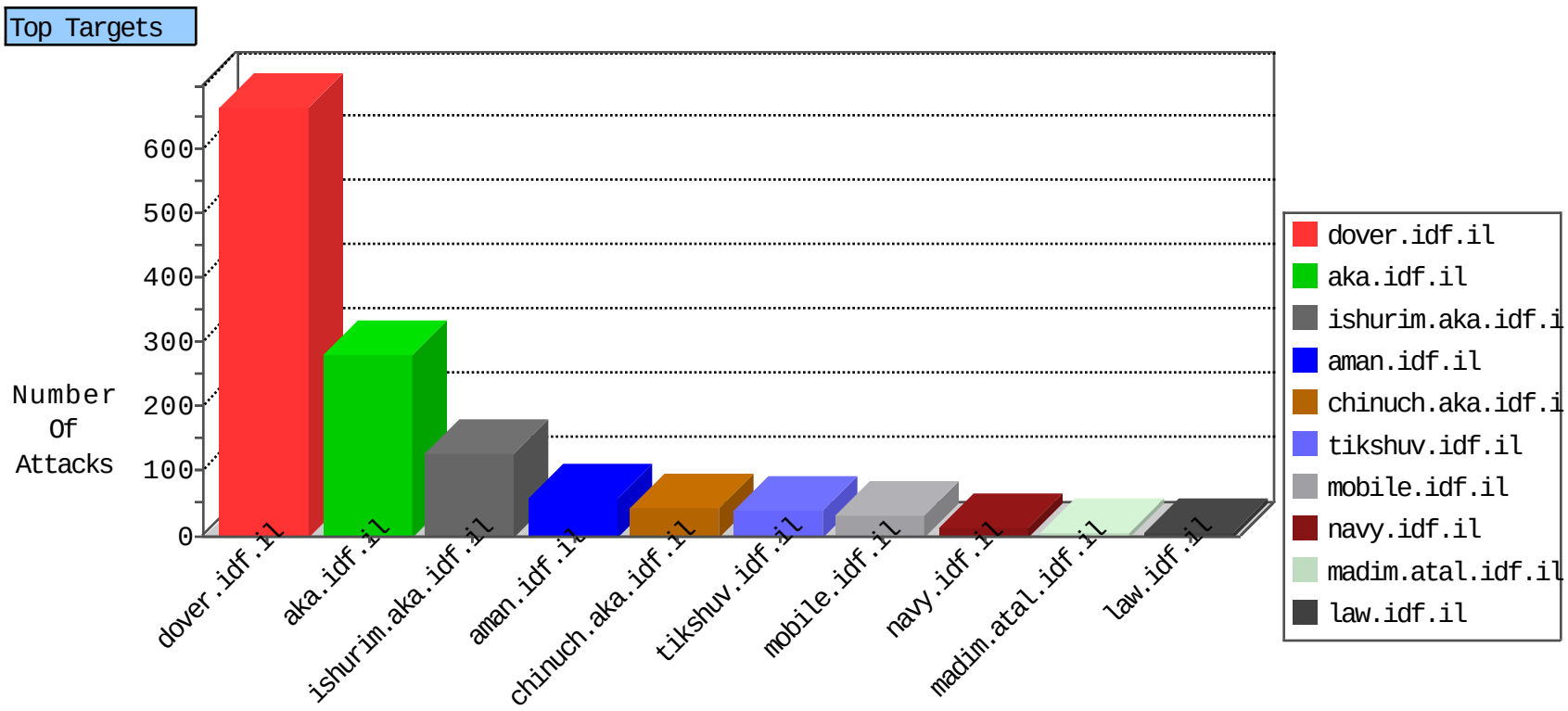
04-28-2016-00:04:01 to 04-28-2016-01:04:01

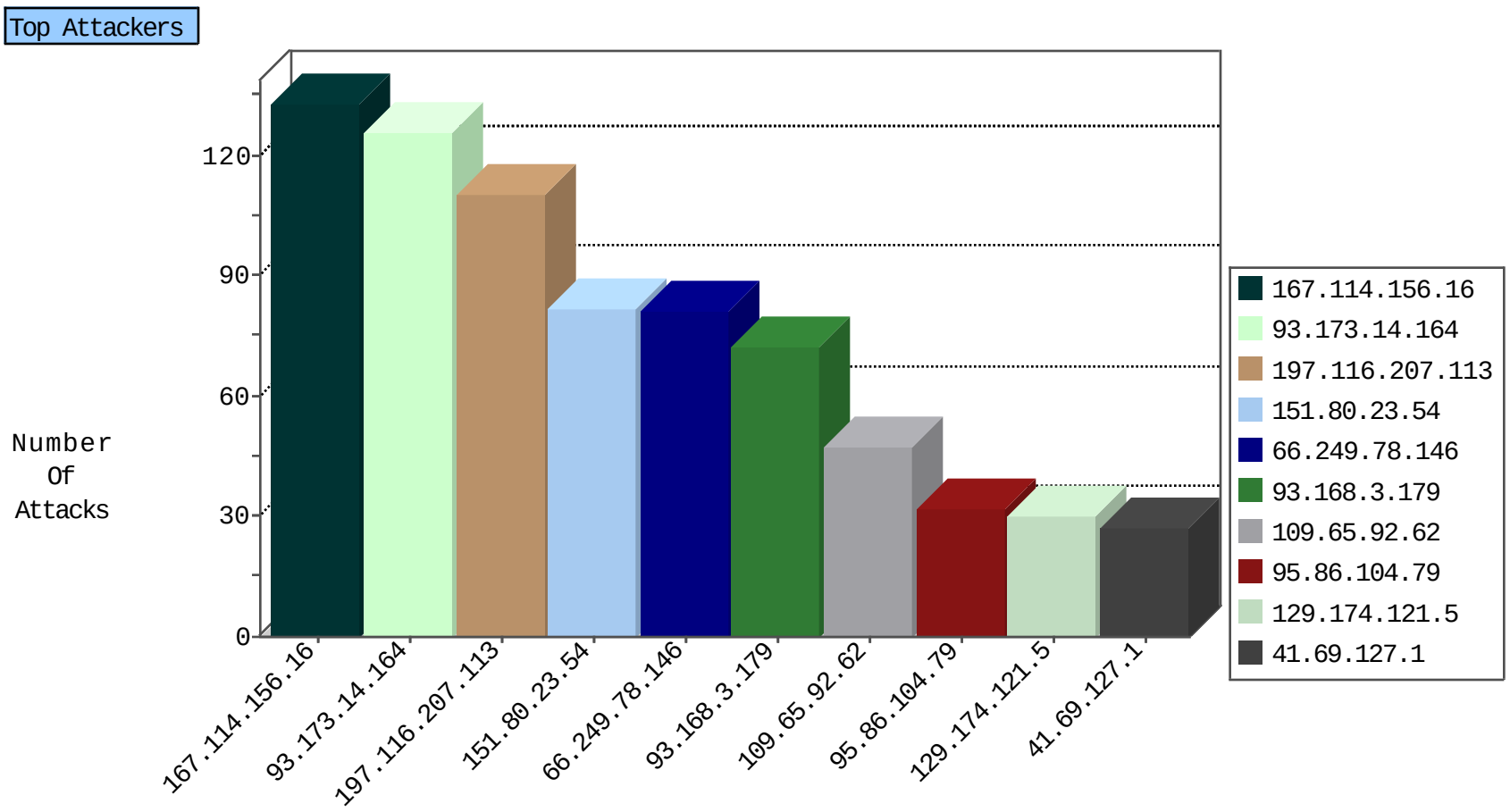
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-28-2016-00:04:01 to 04-28-2016-01:04:01

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	5126
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	84
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3
185.130.5.48	Lithuania	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.48	Lithuania	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
31.148.219.200	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
37.26.146.204	Israel	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

04-28-2016-00:04:01 to 04-28-2016-01:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
187.167.253.1	Mexico	147.237.77.74	law.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
187.167.253.1	Mexico	147.237.77.176	matpash.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

04-28-2016-00:04:01 to 04-28-2016-01:04:01

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	4
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
104.219.238.10	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.149.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.74	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
106.38.241.106	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.214.34.99	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.151.52.231	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.230.74	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
208.167.254.99	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

04-28-2016-00:04:01 to 04-28-2016-01:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.173.14.164	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	126
197.116.207.113	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	83
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	81
93.168.3.179	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	72
109.65.92.62	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	47
151.80.23.54	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
151.80.23.54	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	41
129.174.121.5	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
41.69.127.1	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
197.116.207.113	Algeria	147.237.77.216	dover.idf.il	drop		drop	25
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
198.58.103.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.130.216.252	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.23.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.190.207.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.0	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
23.249.38.161	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.65.136.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.224.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
37.26.148.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.66.50	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.90.194.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.224.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.186.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
95.86.104.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
188.161.51.188	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.139.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
93.19.21.61	France	147.237.77.216	dover.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
37.8.29.14	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
95.86.104.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
95.86.104.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
86.10.72.71	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
95.86.104.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.205.63.129	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.41.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

04-28-2016-00:04:01 to 04-28-2016-01:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.64.99.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
27.127.173.152	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	4
176.13.19.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.23.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.132	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.68.26.225	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.178.183.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
66.249.64.3	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
87.68.26.225	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
188.73.143.132	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/mobile	Block	1
85.65.71.146	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
90.162.241.7	Spain	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/pniot.aspx.español	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
109.67.37.25	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/sachar/mailbox.aspx	None	1
85.65.71.146	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.65.71.146	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
95.86.84.210	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2065-he/cogat.aspx	Block	1
213.7.199.252	Cyprus	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
109.253.227.73	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/general/mobile	Block	1
87.68.26.225	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 87.68.26.225	Block	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
105.159.218.205	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
77.75.77.17	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/32/	Block	1
46.120.137.11	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
157.55.39.146	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20293-he/dover.asp	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/print.css	Block	1
177.148.181.88	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp	Block	1

04-28-2016-00:04:01 to 04-28-2016-01:04:01