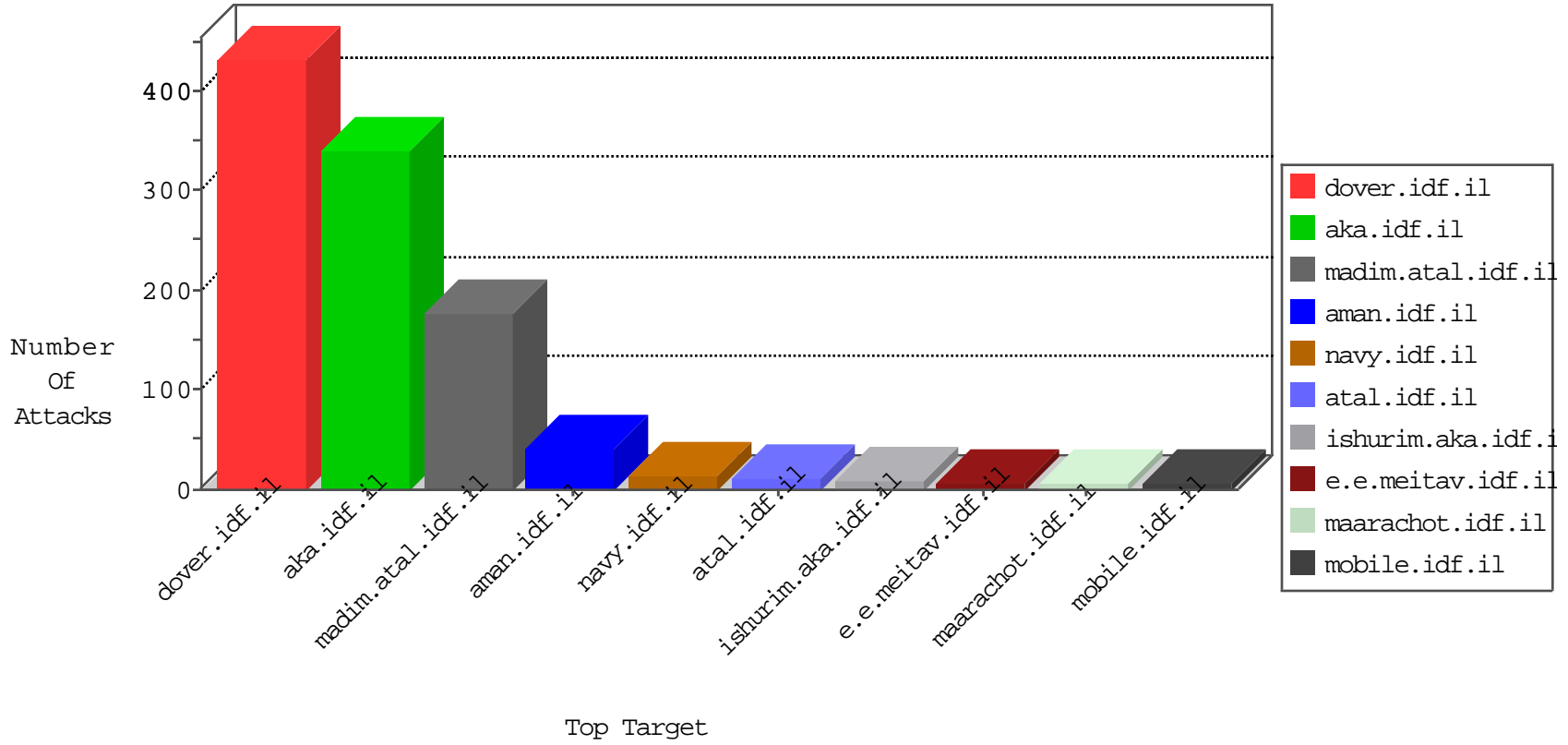


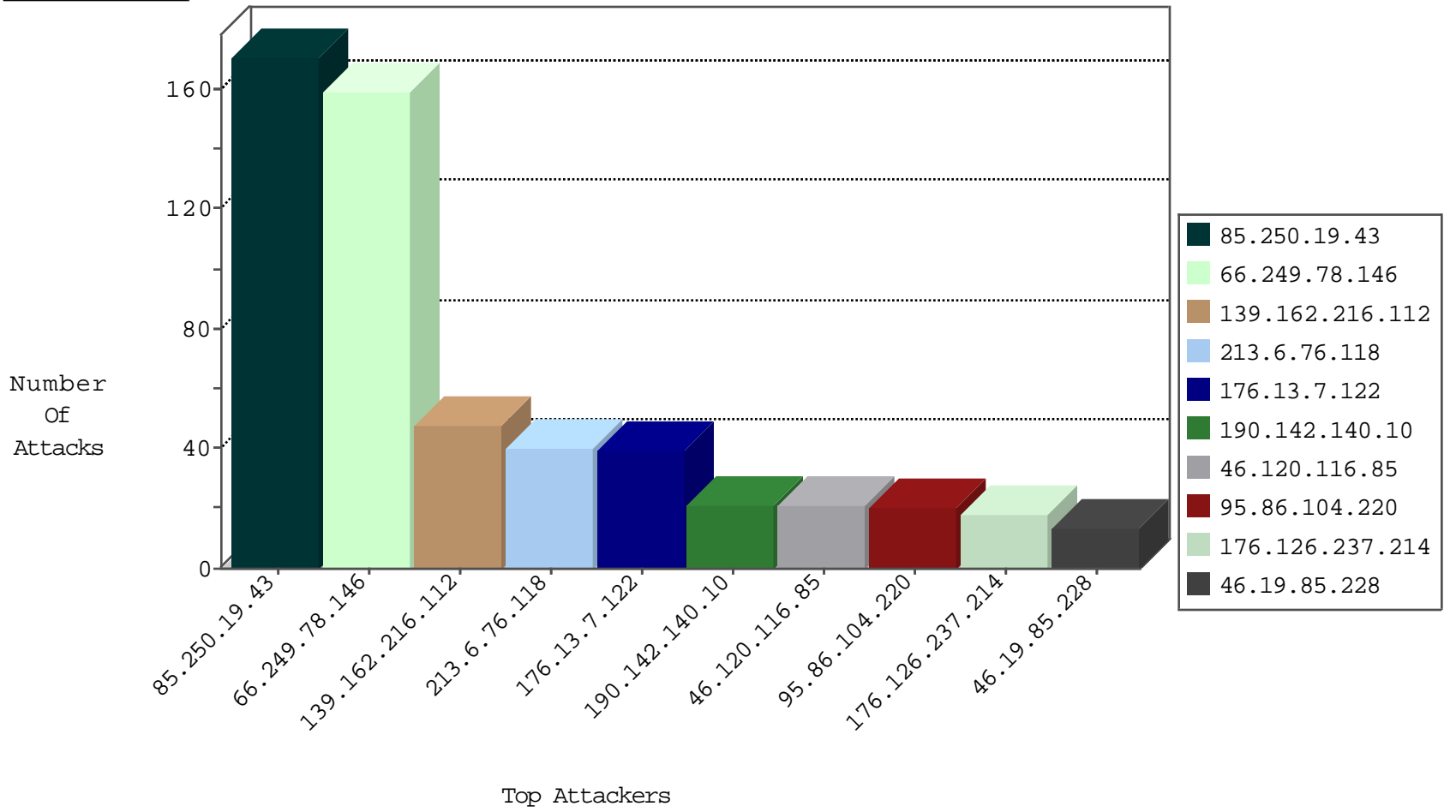
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	TCP handshake violation, first packet not syn	drop	3112
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
69.30.198.148	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
169.54.244.78	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1
74.91.18.42	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
188.138.17.205	France	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
74.91.23.107	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
91.121.79.95	France	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
169.54.244.78	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
74.91.23.107	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	159
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
213.6.76.118	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
176.13.7.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
190.142.140.10	Venezuela	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
46.120.116.85	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
95.86.104.220	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.116.30.23	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
162.243.126.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.84.187.91	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.148.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.7.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.61.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.173.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.226.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.195.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.185	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.0.13.2	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
207.46.13.156	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.55.28.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
84.111.48.211	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.126.237.214	Romania	147.237.76.38	e.e.meitav.idf.	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.130.192.48	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.7	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
72.39.168.87	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.116.251.169	Belgium	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.0.100.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.130.138.150	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.241.229.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.207	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.168.219.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.109.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.29.202.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.250.19.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	171
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	4
80.178.115.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
93.186.31.82	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
93.186.31.114	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.64.194.18	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
93.186.31.97	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.129.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.186.31.81	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
66.249.64.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/masaiyot04112010.aspx	Block	1
132.74.95.21	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/113579.pdf	Block	1
93.186.31.113	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.165.35.15	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
84.94.114.184	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.71	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
66.249.79.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/yoman.asp	Block	1
107.77.95.99	United States	147.237.77.216	dover.idf.il	Malformed URL __atssc=google;2;	Block	1
46.117.62.227	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
74.91.23.107	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.178tx.com/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
141.0.13.2	Norway	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.idf.il/1038-en/dover.aspx	Block	1
41.249.42.19	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
85.64.245.206	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
208.109.252.167	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/test.aspx	Block	1
66.249.79.142	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.79.142	Block	1
46.210.183.99	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1437-he/atal.aspx	Block	1
107.77.95.99	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method okie: in URL __atssc=google	Block	1
93.186.31.96	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.75.78.160	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/33/	Block	1
162.243.188.75	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
93.186.31.114	United Kingdom	147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
46.19.85.1	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.79.142	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/smalim/showbig.aspx	Block	1
46.210.183.99	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
174.129.237.157	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
107.77.95.99	United States	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
46.19.85.20	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
93.186.31.80	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
62.210.254.52	France	147.237.72.166	aka.idf.il	Unknown Parameter amp;rnd in www.aka.idf.il/main/giyus/captcha.ashx	None	1
5.165.35.15	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/faq.aspx	Block	1
93.186.31.98	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
81.218.59.94	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
185.24.76.132	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/edim/yoman/enlarge.asp	Block	1
107.77.95.99	United States	147.237.77.216	dover.idf.il	Illegal HTTP Version __atuvc=3%7C52;_pk_id.20.8afc=82af46ee54a16082.1451246098.1.1451246190.1451246098.;_pk_ref.20.8afc=%5B%22%22%2C%22%22%2C1451246098%2C%22https%3A%2F%2Fwww.google.com%2F%22%5D;ASP.NET_SessionId=p42uz4zvvuezyd453flpcb45	Block	1
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage	Block	1