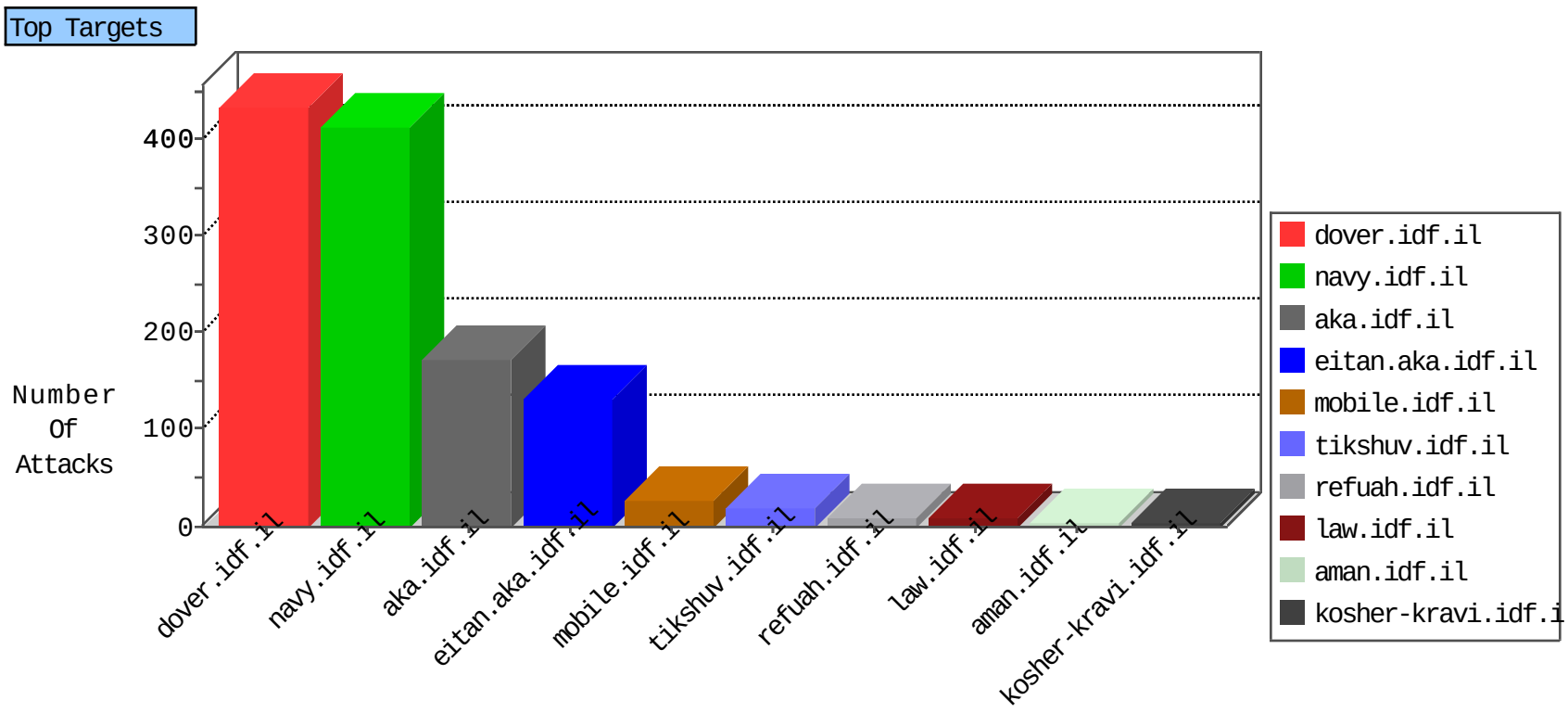
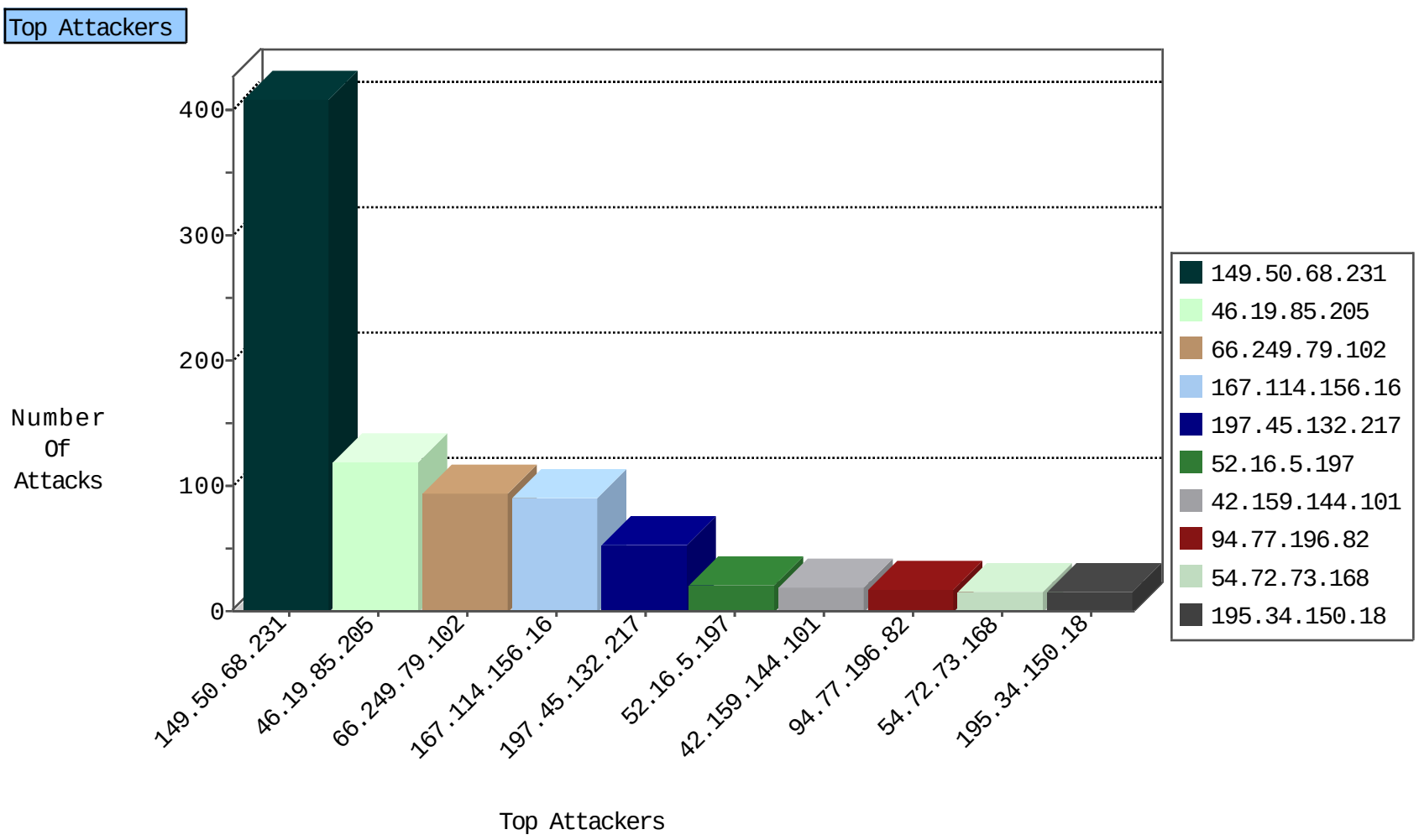
04-30-2016-09:04:01 to 04-30-2016-10:04:01

IDF Under Attack Daily Report





04-30-2016-09:04:01 to 04-30-2016-10:04:01

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	4349
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	325
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
42.159.144.101	China	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	3
42.159.144.101	China	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	2
42.159.144.101	China	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	2
66.240.219.146	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
42.159.144.101	China	147.237.76.86	navy.idf.il	block-sp-traf1	forward	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
42.159.144.101	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
42.159.144.101	China	147.237.76.176	test.ncore.idf.il	JLM_Purple_Con_Limit_Http	drop	1

04-30-2016-09:04:01 to 04-30-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-30-2016-09:04:01 to 04-30-2016-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.50.68.231	147.237.76.86	Israel	navy.idf.il	GPL WEB_SERVER apache directory disclosure attempt	8
149.50.68.231	147.237.76.86	Israel	navy.idf.il	SERVER-WEBAPP apache directory disclosure attempt	8
192.35.222.17	147.237.77.216	United States	dover.idf.il	ET DOS SSL Bomb DoS Attempt	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.79.173	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.165	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
61.182.170.38	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.211	147.237.76.44	China	e.refuah.idf.i	ET SCAN Potential SSH Scan	1
13.92.245.177	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
177.226.38.123	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.100.128	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 2048	1
107.158.255.194	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 3072	1
104.214.25.64	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 3072	1
79.112.42.103	147.237.77.216	Romania	dover.idf.il	Xenu Link Sleuth User Agent	1
58.218.204.211	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
13.92.245.177	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.100.128	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.100.128	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -f -sS	1
113.240.250.154	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
106.184.2.29	147.237.77.61	Japan	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
104.214.25.64	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1

04-30-2016-09:04:01 to 04-30-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.205	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	117
66.249.79.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
52.16.5.197	Ireland	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
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.114	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
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
52.12.123.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.163.234.8	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
128.68.50.185	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.53	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	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.118.116.239	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
94.159.178.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
88.254.110.197	Turkey	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
80.246.136.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.69.217.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.50.68.231	Israel	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
105.103.84.32	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
117.247.193.214	India	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
5.29.121.204	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.50.68.231	Israel	147.237.76.86	navy.idf.il	HTTP Format Sizes	URL length exceeded allowed maximum length of 2048 bytes	monitor	4
66.249.66.177	United States	147.237.77.216	dover.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
128.68.50.185	Russian Federation	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
149.50.68.231	Israel	147.237.76.86	navy.idf.il	Command Injection	command injection detected in URL: 'shadow'	monitor	4
37.46.41.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.146.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.43.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.23.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.151.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.205.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
133.130.158.207	Japan	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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

04-30-2016-09:04:01 to 04-30-2016-10:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.50.68.231	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 149.50.68.231	Block	372
176.13.13.155	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	11
149.50.68.231	Israel	147.237.76.86	navy.idf.il	Multiple Abnormally Long Request from 149.50.68.231	Block	10
217.132.96.204	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	4
149.88.195.82	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	3
95.170.192.221	Iraq	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.170.192.221	Block	3
149.78.93.186	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sachcar	Block	3
109.253.130.134	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1043-h	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
66.249.79.102	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docId in www.aka.idf.il/brothers/klali/default.asp	None	1
42.159.144.101	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to g-ecx.images-amazon.com/images/g/01/x-locale/common/transparent-pixel._cb386942464_.gif	Block	1
149.78.151.199	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
85.25.103.119	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
54.203.240.108	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/registrationwizard/register.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
2.53.29.11	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.249.79.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
52.12.14.230	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/klali.aspx	Block	1
87.70.109.55	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1239-he/atal.aspx	Block	1
54.214.82.219	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/forgotpassword.aspx	Block	1
31.151.198.129	Netherlands	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.151.198.129	Block	1
79.180.177.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
52.12.91.186	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1093-7963-he/מא ירשתמו|.aspx	Block	1
89.138.48.208	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
220.255.219.5	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
31.151.198.129	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
80.153.42.47	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
52.13.45.110	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/faq.aspx	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
42.159.144.101	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to g-ecx.images-amazon.com/images/g/01/x-locale/common/transparent-pixel._cb386942464_.gif	Block	1
80.246.136.57	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
54.188.243.44	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/klali.aspx	Block	1
2.53.29.11	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
95.170.192.221	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1

04-30-2016-09:04:01 to 04-30-2016-10:04:01