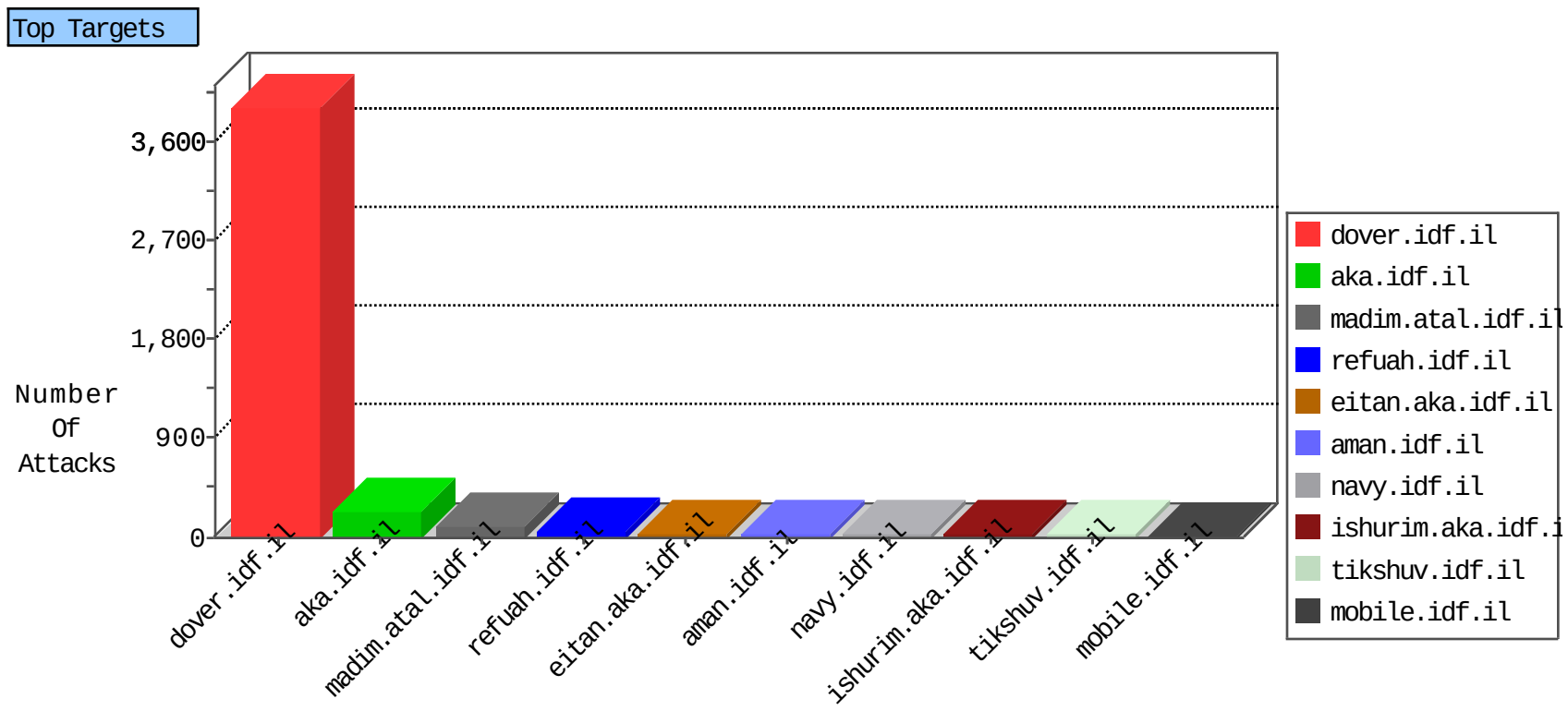
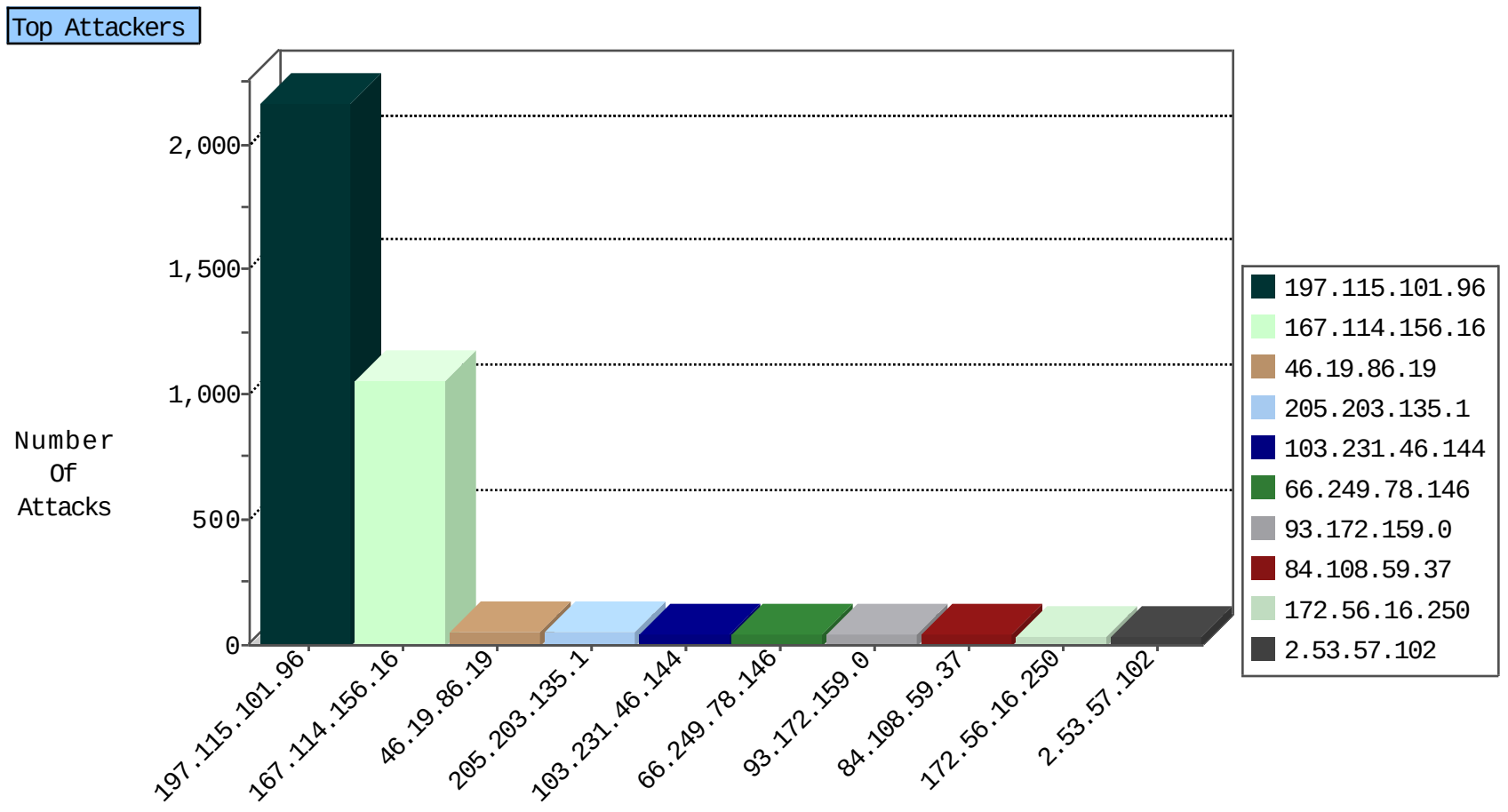
04-27-2016-18:04:08 to 04-27-2016-19:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-27-2016-18:04:08 to 04-27-2016-19:04:08

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	DOS-Tool-SwitchbladG	dest-reset	448
192.164.241.72	Austria	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	5
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
80.82.78.38	Netherlands	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
80.82.78.38	Netherlands	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	2

04-27-2016-18:04:08 to 04-27-2016-19:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	2
5.43.221.172	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1

04-27-2016-18:04:08 to 04-27-2016-19:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
103.231.46.144	147.237.77.216	India	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	42
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
91.201.236.158	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
80.82.78.38	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
67.79.37.250	147.237.76.30	United States	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
122.164.100.104	147.237.76.30	India	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.158	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.0.35	Ukraine	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.0.15	Netherlands	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
104.214.25.64	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1

04-27-2016-18:04:08 to 04-27-2016-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1620
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	962
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	drop		drop	434
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	108
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
84.108.59.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
79.177.123.178	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
2.53.15.40	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.178.255.226	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.53.57.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
82.196.42.196	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
199.58.86.211	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
172.56.16.250	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
69.27.151.62	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
37.26.148.246	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.205	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
88.172.156.221	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
172.56.16.250	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.28.131.108	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
200.128.7.98	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
87.70.79.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
69.248.129.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.27.105.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
128.72.212.131	Russian Federation	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
79.177.178.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
172.56.16.250	United States	147.237.77.216	dover.idf.il	SYN Attack		reject	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.177.178.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.55.17.211	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
93.172.159.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
80.246.137.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
81.218.241.26	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	4
109.253.226.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
31.210.176.149	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	3
109.253.223.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	2
80.246.136.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.57	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.71.31.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.136.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
23.81.90.154	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
67.79.37.250	United States	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.65.232	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/shared/clientscripts/swfobject.js	Block	1
177.102.18.225	Brazil	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 177.102.18.225	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
123.59.59.52	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.mafengwo.cn/main/home/default.aspx	Block	1
83.68.225.42	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dail'a=0	Block	1
79.182.43.91	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/general/mobile	Block	1
66.249.65.239	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
177.102.18.225	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/portuguese/	Block	1
109.64.225.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl57 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/key/aswd56425csa	Block	1
84.108.59.37	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
80.82.78.38	Netherlands	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
180.76.15.161	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8905-he/refuah.aspx	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
149.78.136.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.250.105.188	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl50.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
80.82.78.38	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
197.115.101.96	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmorret	Block	1
109.253.226.215	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.22.131.105	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	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/6/size338x0/1796.jpg	Block	1
46.116.40.129	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/contactus/mobile	Block	1
157.55.39.13	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1