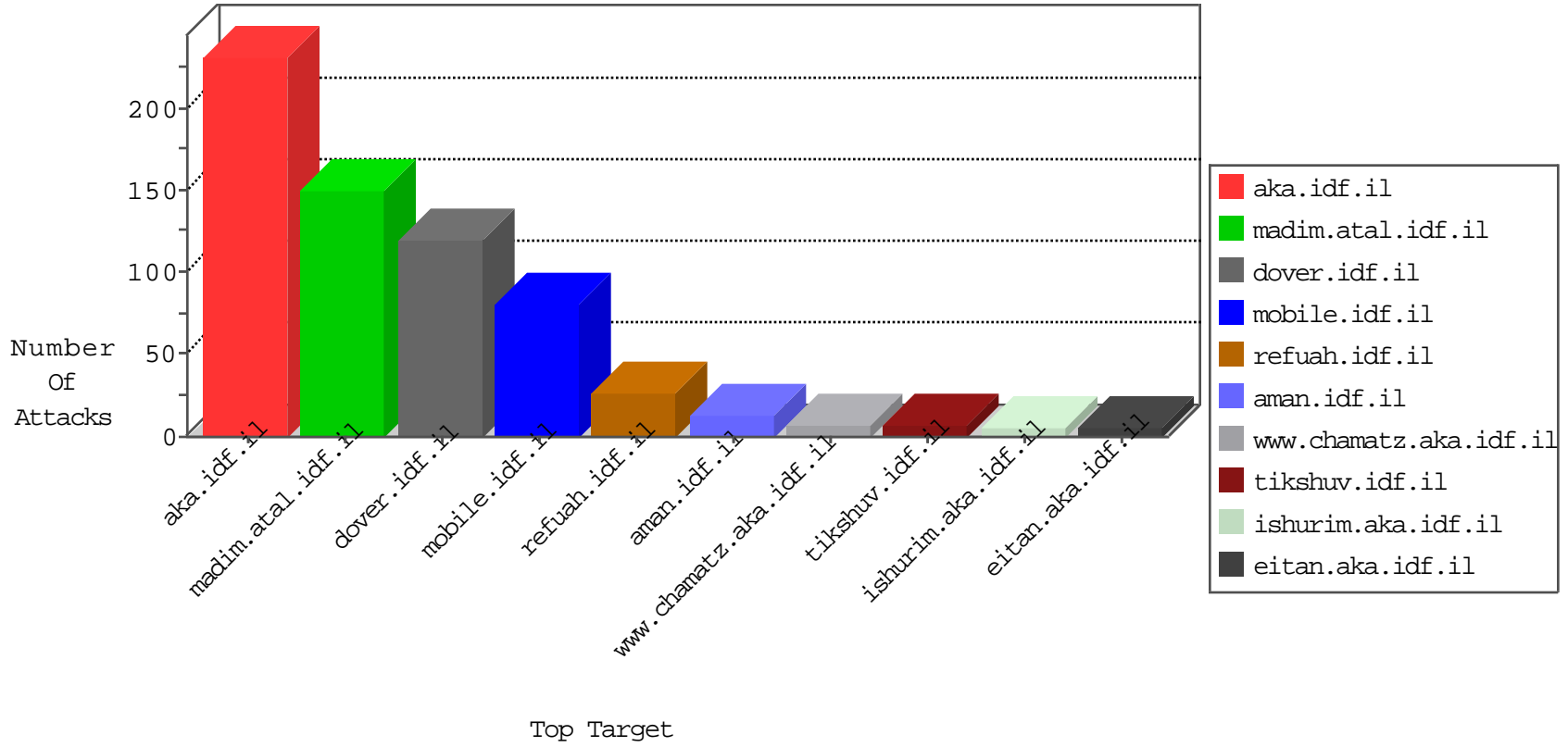


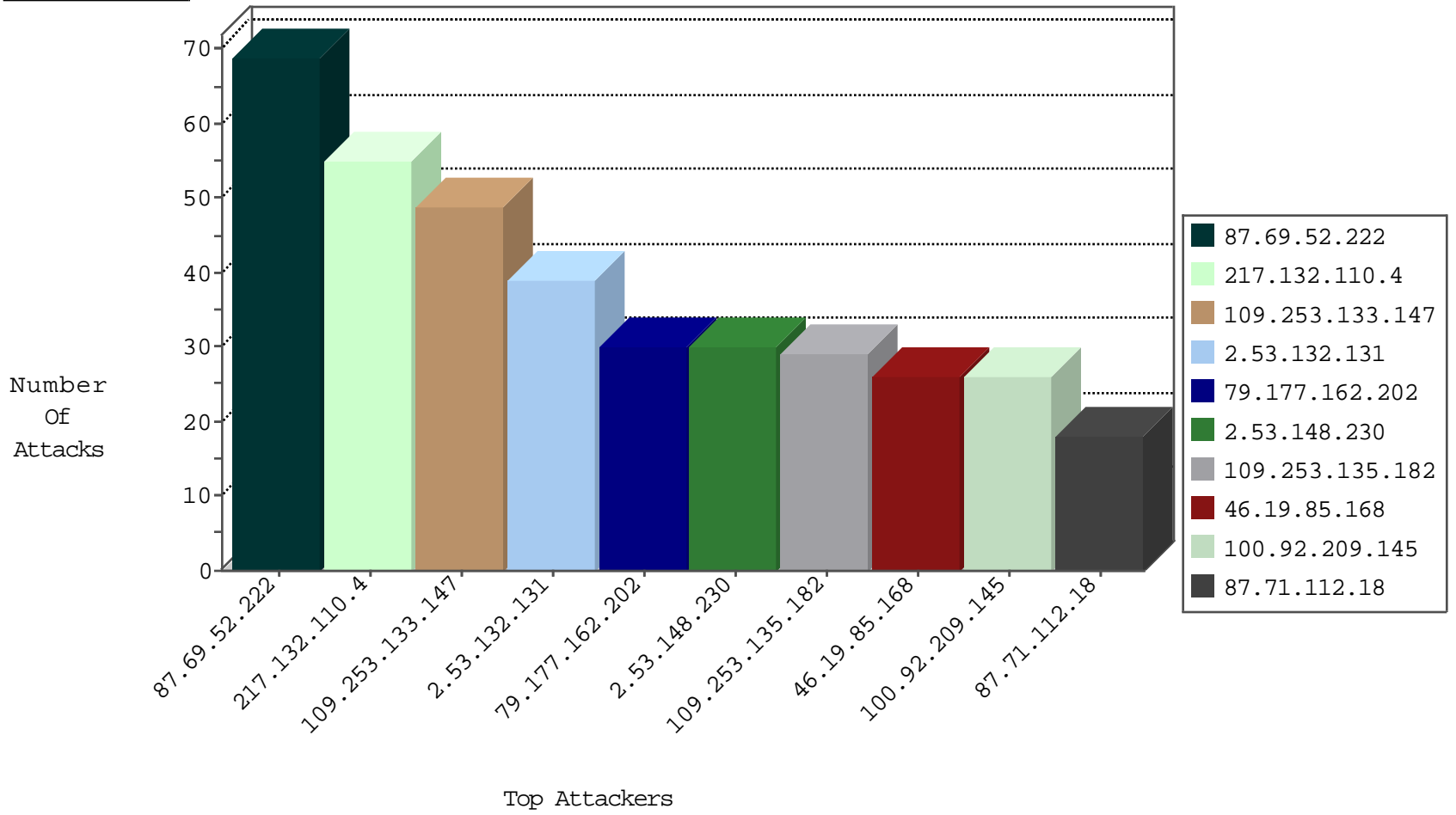
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.14	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
84.94.75.254	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
160.80.221.37	Italy	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
37.26.149.185	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	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
46.227.67.158	147.237.8.28	Sweden	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.72.167	United States	ishurim.aka.idf.il	ET DROP Dshield Block Listed Source	1
179.43.141.228	147.237.77.176	Switzerland	matpash.idf.il	ET SCAN Potential SSH Scan	1
124.123.236.46	147.237.77.19	India	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.3	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
104.232.98.3	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
61.161.168.27	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.73	147.237.72.167	Ukraine	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.72.167	Japan	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
119.140.5.184	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.3	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
93.173.122.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.69.52.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	37
87.69.52.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	32
2.53.148.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
79.177.162.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
217.132.110.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
100.92.209.145		147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
217.132.110.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	10
46.19.85.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
100.92.209.145		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.132.110.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.24.207.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
217.132.110.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
84.229.10.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
77.138.106.77	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
217.132.110.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.34	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.147.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.120.168.248	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
185.120.124.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.40.139.39	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.138.106.77	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.229.10.5	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.3.147.249	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.55.170.30	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.236	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
185.24.207.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.168	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.66	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.4.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
77.138.106.77	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.46.41.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.127.51.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.62.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.64.126.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.19.86.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
117.208.69.91	India	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
100.92.209.145		147.237.76.39	mobile.meitav.idf.il	drop	First packet isn't SYN	drop	2
89.138.249.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
46.19.86.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.133.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
2.53.132.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
109.253.135.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
87.71.112.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
82.81.103.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
85.65.149.230	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.149.230	Block	5
109.67.209.227	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.67.209.227	Block	4
109.67.243.124	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	4
84.108.136.139	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
109.67.209.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authenticationervice.aspx/getauthuser	Block	2
46.121.197.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.137.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.176.178	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
66.102.9.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
185.32.179.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/63578.doc	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
46.19.86.176	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
114.98.244.254	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar/cogat.aspx/trackback/	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyus/forum/asp/showforum.asp	Block	1
201.137.183.138	Mexico	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
157.55.39.102	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
85.65.149.230	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/kiosk/kiosk.aspx	Block	1
77.237.138.202	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
213.57.154.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
84.111.242.94	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19478-he/idfgdover.asp	Block	1
66.102.6.140	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
176.13.1.46	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
85.64.113.49	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 85.64.113.49	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
185.32.179.8	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.32.179.8	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
85.64.113.49	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/news/news.in.aspx	Block	1