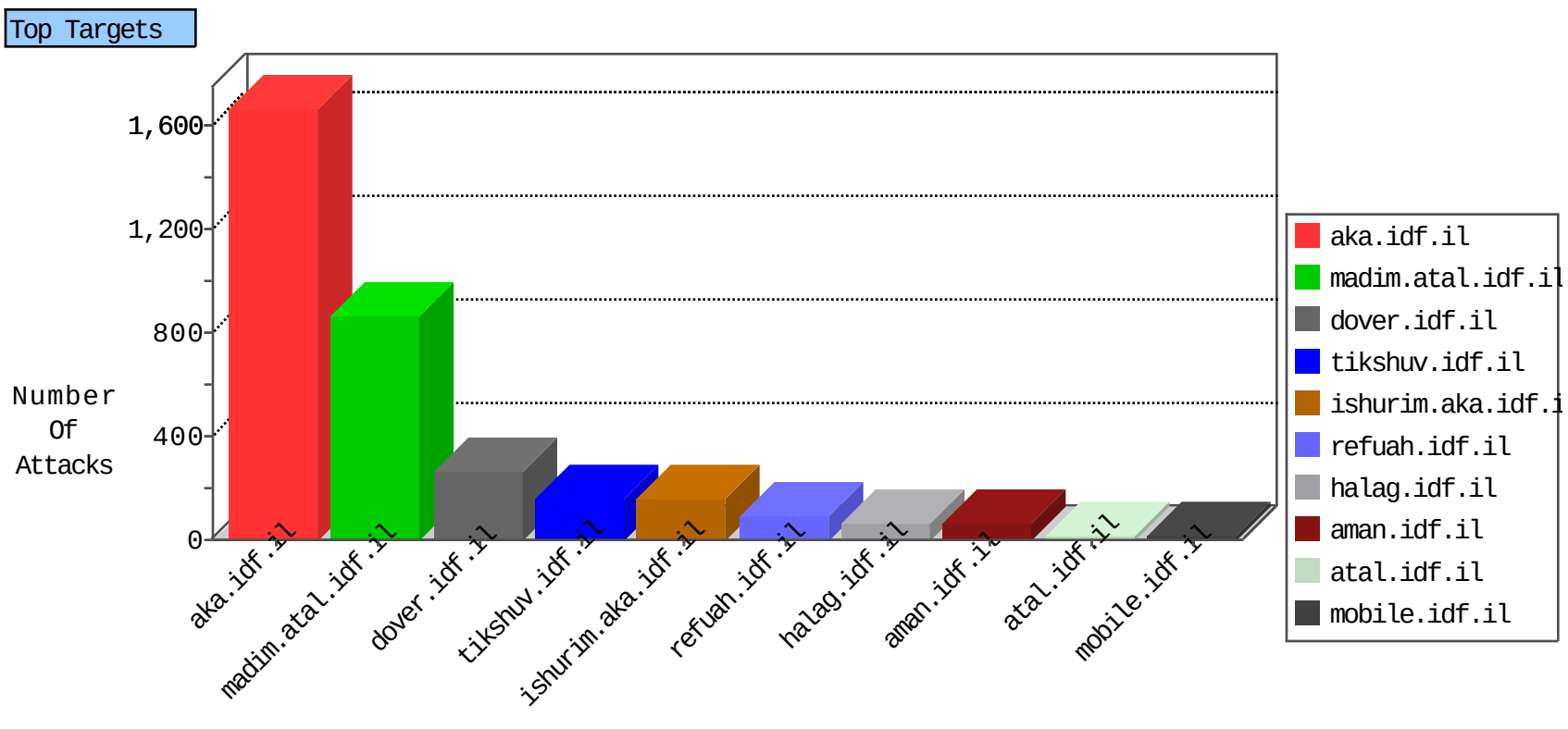
02-03-2016-11:04:01 to 02-03-2016-12:04:01

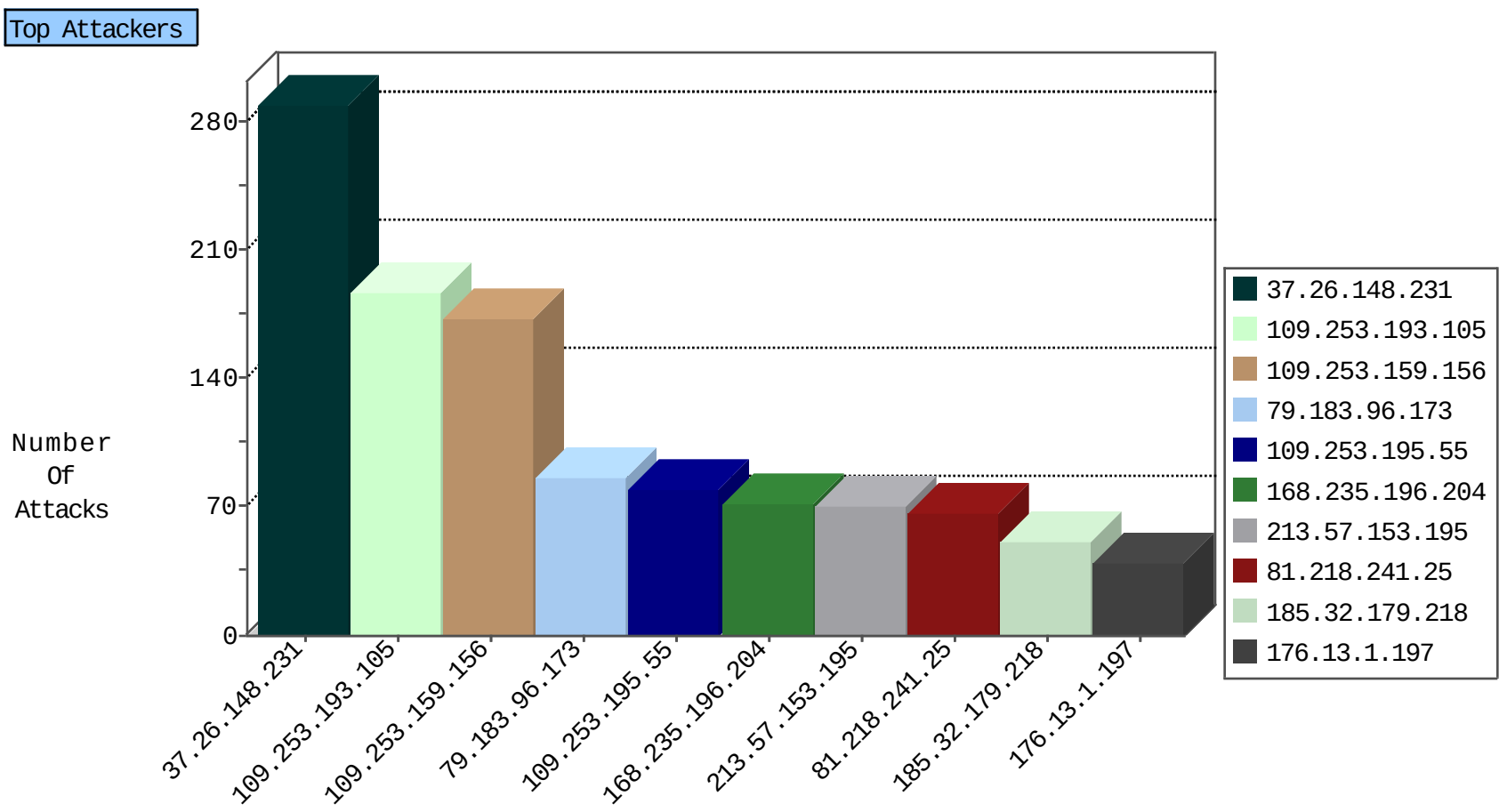
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-03-2016-11:04:01 to 02-03-2016-12:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	210
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	81
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
157.55.39.140	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
168.235.196.204	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
201.190.37.43	Honduras	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
201.190.37.43	Honduras	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

02-03-2016-11:04:01 to 02-03-2016-12:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

02-03-2016-11:04:01 to 02-03-2016-12:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.222.185.165	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
109.253.199.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.193.105	147.237.0.19	Israel	madim.atal.idf.il	GPL SCAN myscan	1
79.180.162.132	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.1.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.153.195	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.51.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.19	United States	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
31.154.21.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.144.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.222.185.165	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
149.78.199.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.193.105	147.237.0.19	Israel	madim.atal.idf.il	INDICATOR-SCAN myscan	1
92.225.105.214	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.67.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.216.2.13	147.237.76.39	Taiwan	mobile.meitav.idf.i	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
212.199.152.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.118.78.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
168.235.196.204	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

02-03-2016-11:04:01 to 02-03-2016-12:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.196.204	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	69
176.13.1.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
132.72.89.130	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	26
62.128.48.158	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
149.20.63.13	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
85.65.236.70	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
2.52.154.14	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.19.85.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
46.19.85.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.54.50.59	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
109.253.207.21	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
41.189.228.53	Djibouti	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
81.218.179.41	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.85.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.182.164.48	Israel	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
41.189.228.53	Djibouti	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.39.6	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.150.97.225	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
82.166.77.241	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
2.52.189.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.39.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.106.46.74	Palestinian Territory, Occupied	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.39.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.3.146.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.117.143.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.178.146.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.39.6	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
2.54.183.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.22.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.193.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.194.199.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.189.228.53	Djibouti	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
94.230.86.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.189.228.53	Djibouti	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.52.31.156	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.227	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	160
37.26.148.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
109.253.193.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
109.253.159.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	94
79.183.96.173	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
109.253.193.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	83
109.253.195.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
213.57.153.195	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	70
109.253.159.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	56
185.32.179.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
2.54.28.98	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	31
176.13.14.69	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
87.68.246.247	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	20
109.253.159.156	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.159.156	Block	20
46.19.85.178	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
80.74.110.141	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	20
46.19.85.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
149.50.94.236	United States	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
109.253.211.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	15
87.69.1.22	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
132.68.176.199	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
37.26.148.231	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.148.231	Block	12
79.183.18.140	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
176.13.13.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.19.86.221	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
46.19.86.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
5.29.38.98	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
87.68.72.226	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
79.182.200.127	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
109.253.137.226	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	9
2.54.132.66	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
2.52.59.100	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
31.168.13.78	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	8
31.168.71.19	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
37.26.147.209	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
2.54.37.24	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
82.166.77.241	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
2.52.31.101	Israel	147.237.72.167	ishurim.aka.idf.i	Distributed Too Many of the Same Response Code (404)	Block	7
31.210.186.95	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
212.143.161.239	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
109.253.144.211	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
46.19.85.13	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
80.246.138.238	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
109.64.130.122	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
213.8.204.28	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
80.246.140.193	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
176.13.20.127	Israel	147.237.72.166	aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6

02-03-2016-11:04:01 to 02-03-2016-12:04:01