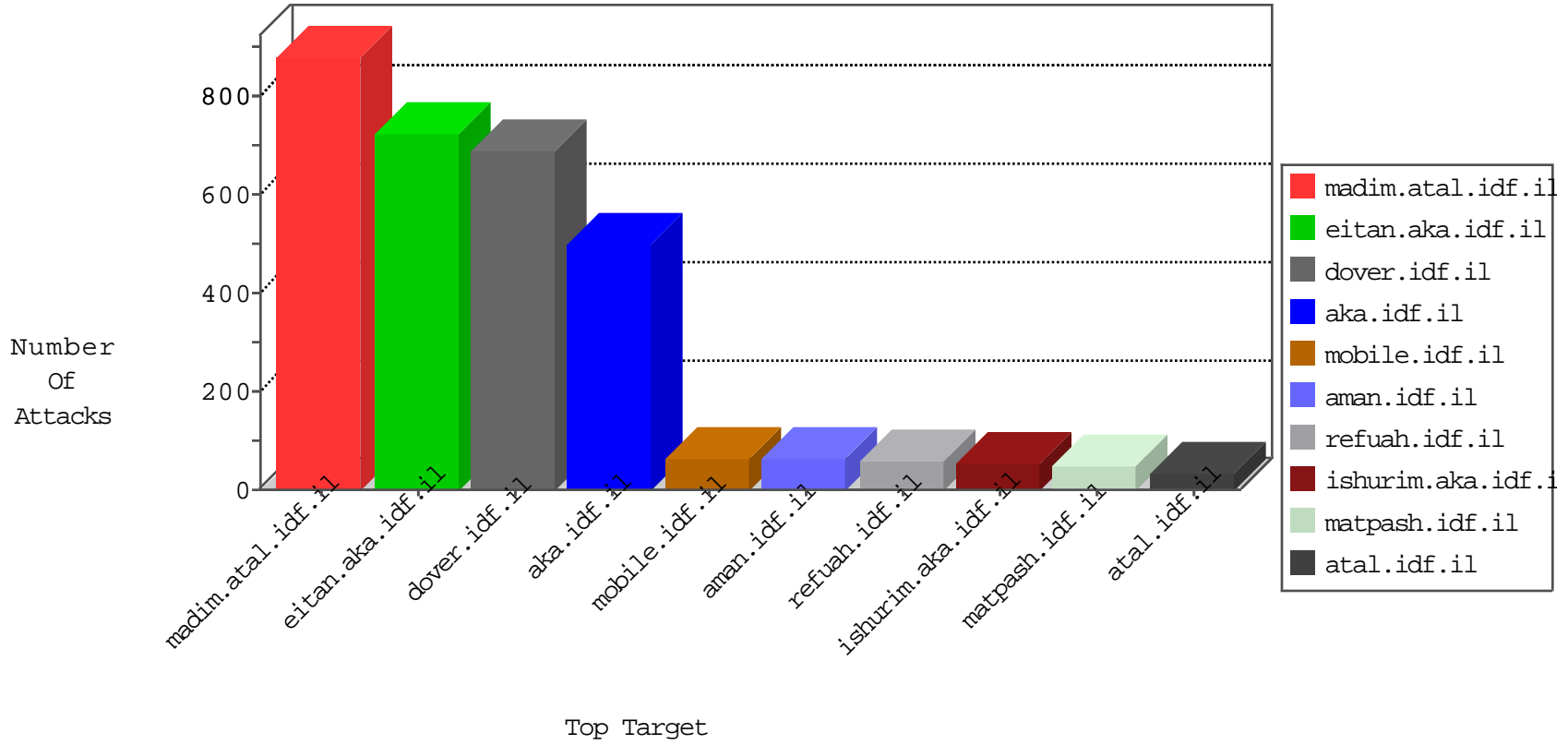


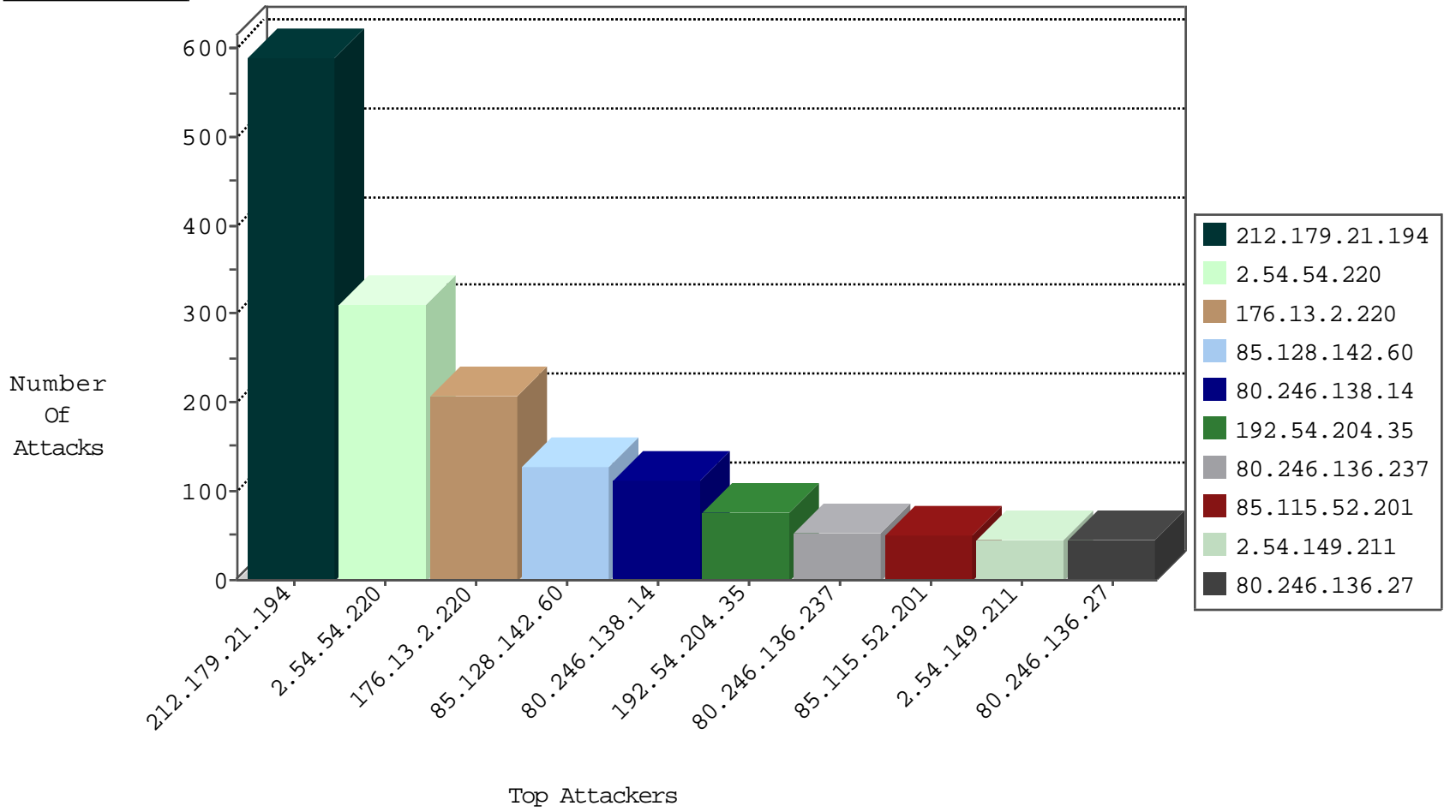
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.201	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	20
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1
104.192.0.226	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
104.192.0.226	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.188.161.145	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
84.109.0.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.159.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.68.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.191.249.36	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
2.54.55.22	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.60.218	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
188.214.128.12	147.237.0.19	Romania	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
132.72.229.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.163.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.219.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.253.96.122	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
220.191.249.36	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
5.29.244.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.68.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.151.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
173.61.25.231	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	316
85.128.142.60	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	128
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
100.100.76.253		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
82.80.54.124	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
108.205.248.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
46.19.86.166	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	23
46.244.90.208	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
40.77.167.104	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
2.54.149.211	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.19.85.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
117.136.40.129	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.85	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
85.115.52.201	United Kingdom	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
80.246.130.230	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
192.54.204.35	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
100.100.70.245		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.7.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
70.208.64.249	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.126.119		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
17.78.165.143	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
37.26.147.254	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.99.251	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
213.8.122.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	8
2.54.54.220	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
109.186.162.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.54.146.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
149.88.38.117	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
109.186.162.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.64.112.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
190.224.233.114	Argentina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.149.211	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.149.211	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
2.54.149.211	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.149.211	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.126	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.139.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.57.200	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.110.40.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.18.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.242	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	265
2.54.54.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	156
2.54.54.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
176.13.2.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
176.13.2.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	100
80.246.138.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
192.54.204.35	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	61
80.246.136.237	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
80.246.136.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	44
80.246.138.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	43
2.54.54.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	41
85.115.52.201	United Kingdom	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
176.12.143.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
80.246.137.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	20
80.246.136.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	15
80.246.137.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
80.246.137.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
2.54.141.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
80.246.136.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.66.141.26	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.141.26	Block	5
80.246.137.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
94.159.179.229	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
37.142.171.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	4
84.132.1.11	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	4
79.180.228.171	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
37.142.224.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mail/sachar	Block	4
176.13.18.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
62.90.163.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	3
80.246.137.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	3
80.246.136.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.188.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.198	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/shared/clienthttp/1.1 200 okdate: mon, 16 nov 2015 09:21:49 gmtime: wed, 12 dec 2012 05:52:44 gmtime:	Block	3
80.246.137.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.22.129.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.137.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.137.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.22.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
50.18.94.121	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus	Block	2
80.246.136.69	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	2
109.186.51.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.137.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.23	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
213.57.126.231	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/ufi/reaction/	Block	2
176.12.140.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.137.153	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2