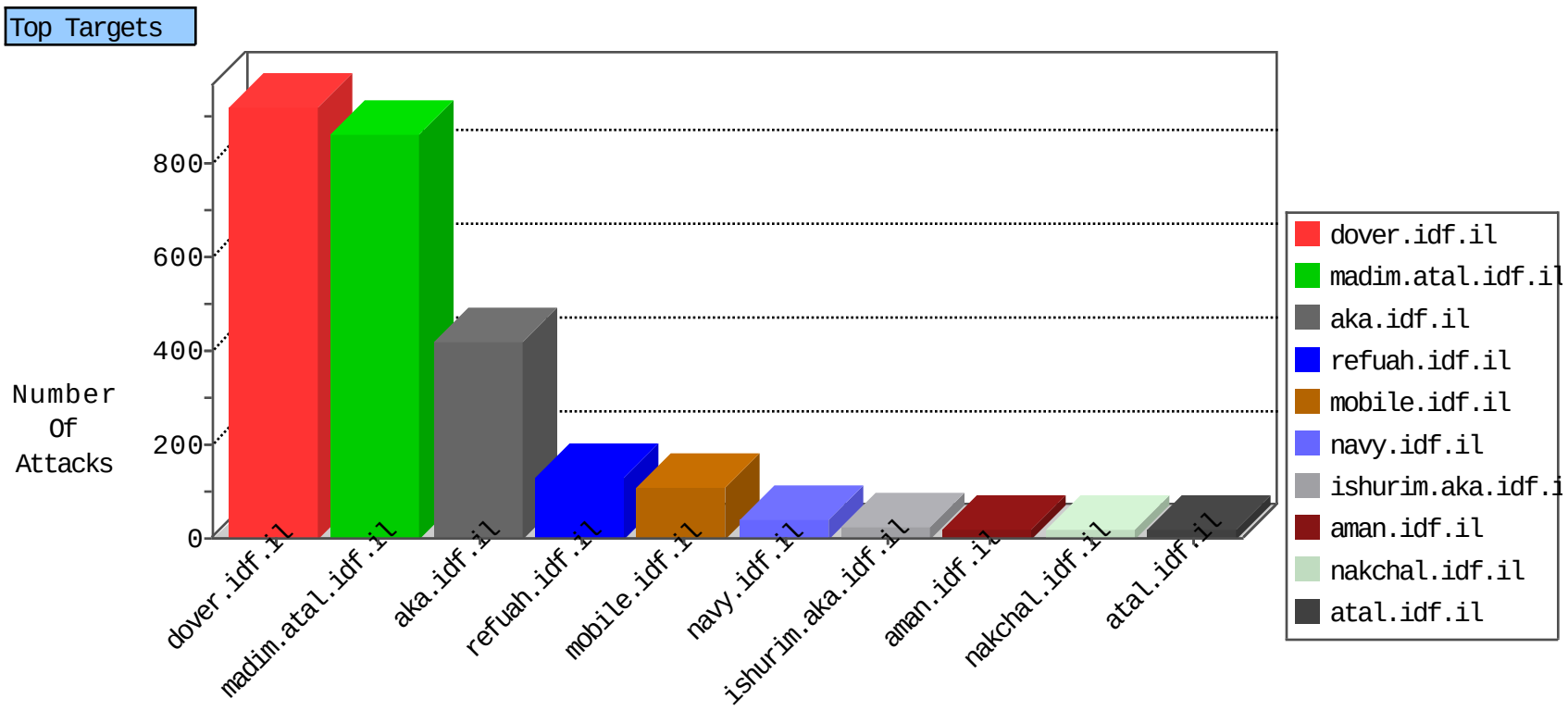
05-01-2016-14:04:05 to 05-01-2016-15:04:05

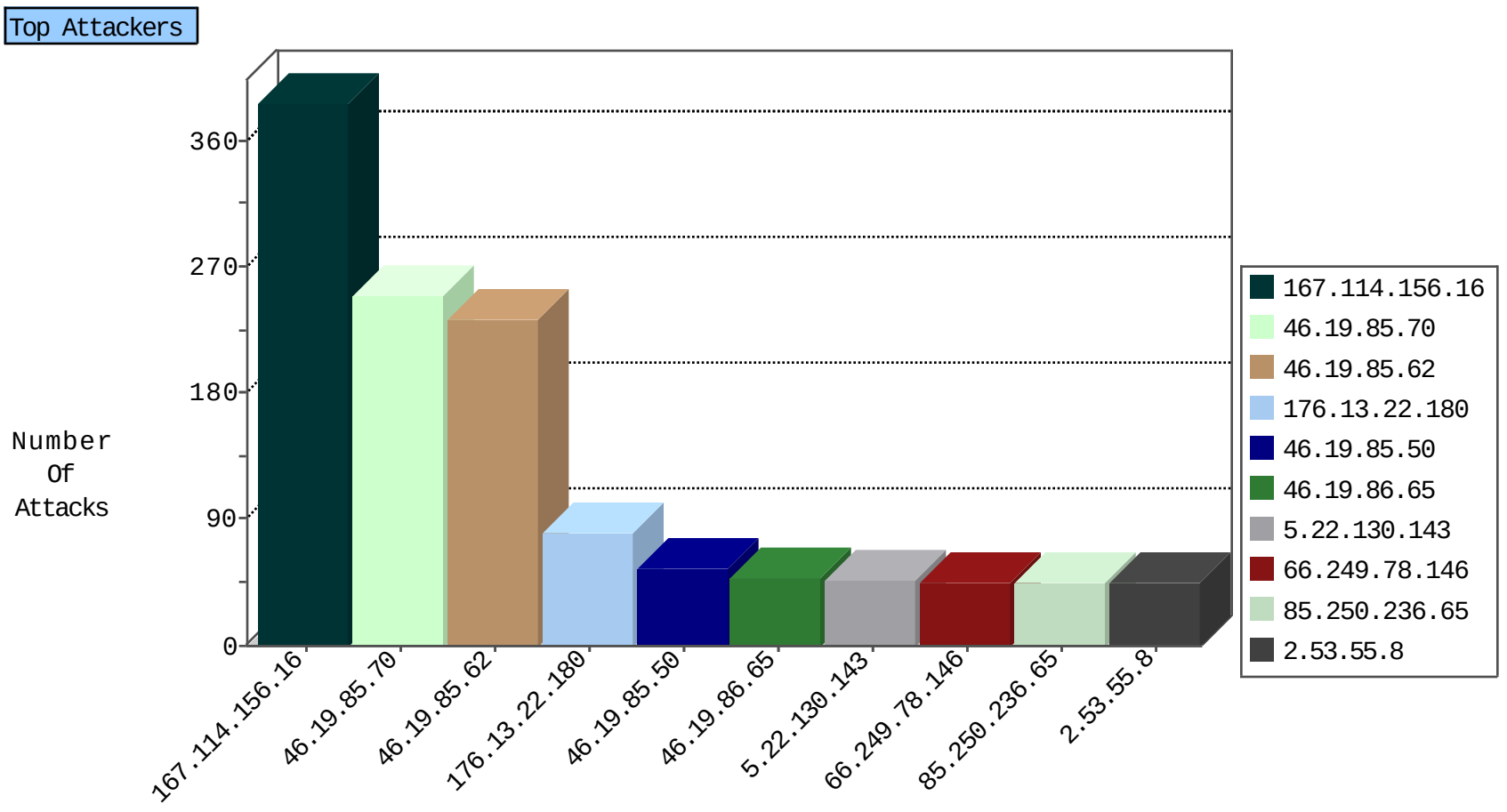
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

05-01-2016-14:04:05 to 05-01-2016-15:04:05

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	14097
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4546
217.132.34.164	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	203
212.143.211.200	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	105
2.53.63.253	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
2.55.136.107	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.181.98.48	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.64.5.154	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4
109.253.195.179	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
2.55.164.16	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
109.253.214.208	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
84.95.21.211	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
192.168.0.8		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	2
185.32.179.62	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
185.120.125.123	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.117.12.44	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
2.53.141.32	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.253.214.208	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
119.40.100.114	Mongolia	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.94.111.1	Russian Federation	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

05-01-2016-14:04:05 to 05-01-2016-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-01-2016-14:04:05 to 05-01-2016-15:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.166.197.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.251.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.206.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.105.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
2.55.152.0	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.15.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
163.172.8.19	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.201.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.197.72.206	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.163.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.169.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.97.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.21.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
176.13.10.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.50.74.179	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
104.214.34.99	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
95.86.120.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

05-01-2016-14:04:05 to 05-01-2016-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
5.22.130.143	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
178.25.1.130	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
77.235.135.88	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
2.53.29.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
85.250.236.65	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.85.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.13.15.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.250.236.65	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
37.26.146.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
123.103.8.100	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.178.83.218	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
85.250.236.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.8.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.1.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.132.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.250.236.65	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
94.230.86.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.8.204.58	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.86.179	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
123.103.8.112	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.179.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.34	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.102.242.200	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.95.206.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.10.211	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.134.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.204.140	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.120.125.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.81	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.204.140	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

05-01-2016-14:04:05 to 05-01-2016-15:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	249
46.19.85.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	232
176.13.22.180	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
2.53.55.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
46.19.85.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
80.246.136.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
46.210.186.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
46.19.85.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
2.53.25.54	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
80.246.136.111	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.136.111	Block	9
176.13.2.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
176.43.145.117	Turkey	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.43.145.117	Block	6
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	6
176.43.145.117	Turkey	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
31.154.41.17	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	5
2.55.48.20	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	5
46.19.86.113	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	5
2.55.141.72	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	4
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	4
109.253.132.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
185.32.179.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.32.179.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.62	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.211	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.248.253.133	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1556-en/	Block	3
2.53.29.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
194.9.252.237	United Kingdom	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.3.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
138.134.102.15	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 138.134.102.15	Block	2
46.19.86.41	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.142.72.86	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
157.55.39.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.137.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.8.211	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
176.13.1.19	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
95.86.79.87	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/mobile	Block	2
176.13.15.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.226.44.156	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
192.115.97.253	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109705.pdf	Block	2
109.253.132.60	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
178.137.83.178	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1556-en/	Block	2

05-01-2016-14:04:05 to 05-01-2016-15:04:05