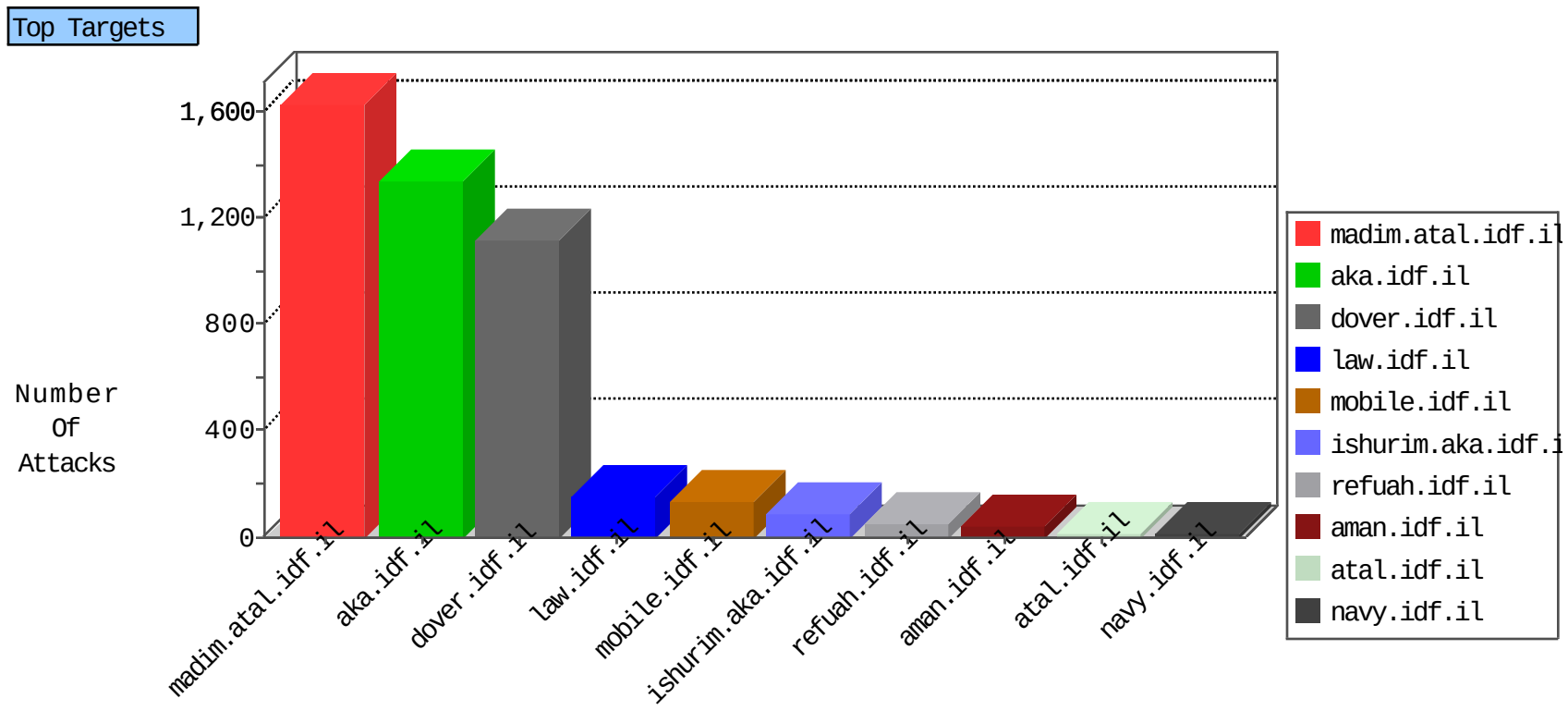
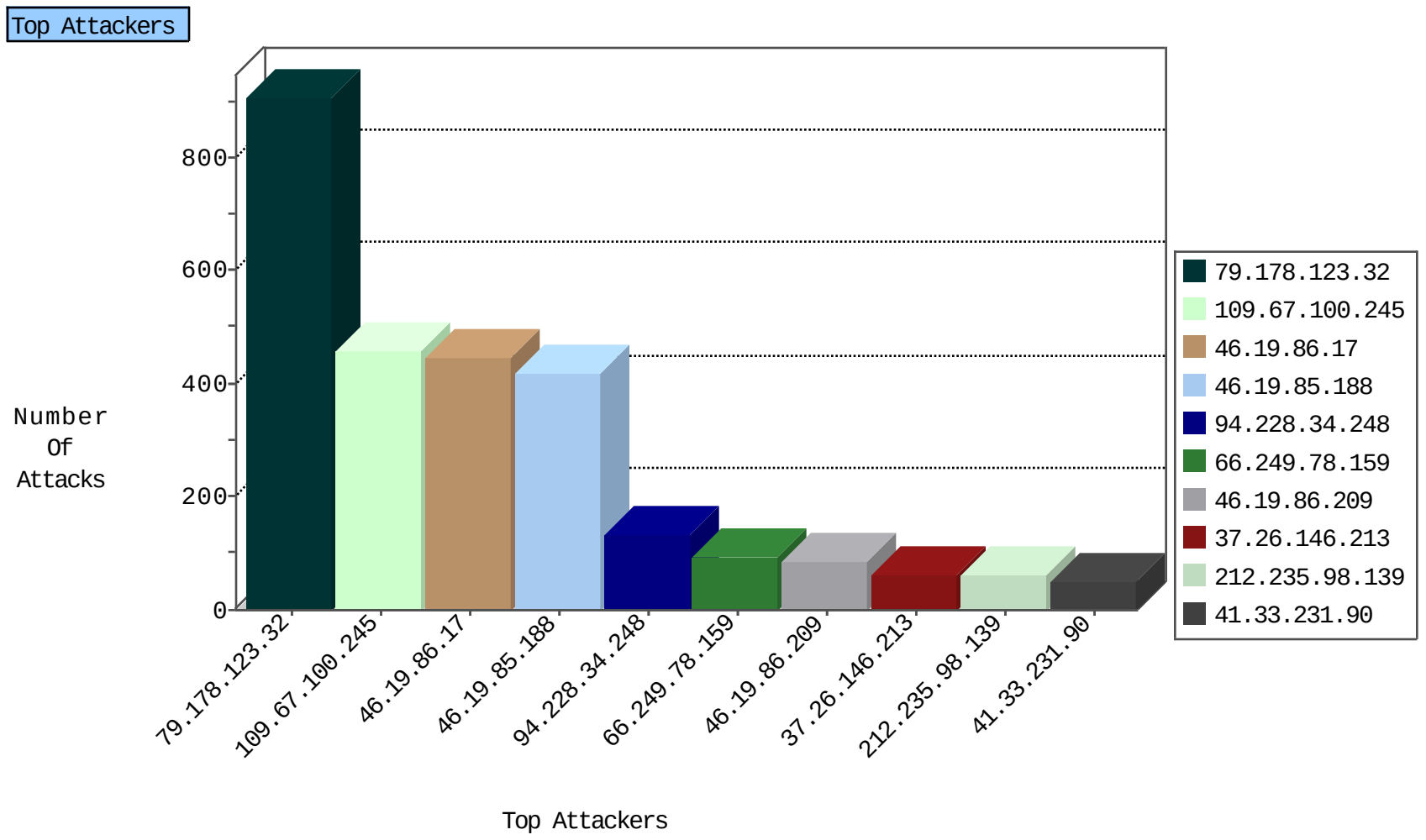
11-22-2015-12:04:06 to 11-22-2015-13:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-22-2015-12:04:06 to 11-22-2015-13:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	753
149.78.228.245	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	166
192.118.30.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	16
87.69.102.202	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
77.125.138.22	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	10
79.182.164.44	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
37.26.147.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
139.0.88.27	Indonesia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
81.218.206.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
147.236.38.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
194.114.146.227	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
132.64.102.64	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.183.21.232	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.179.172.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.180.116.180	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
176.228.176.104	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.93	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-22-2015-12:04:06 to 11-22-2015-13:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.193.51.30	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
79.179.176.46	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3

11-22-2015-12:04:06 to 11-22-2015-13:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
132.64.92.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.114.17.100	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
111.93.198.54	147.237.76.147	India	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
82.166.22.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.22.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.244.22.103	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.204.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.129	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
2.52.184.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.66.161.159	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
122.114.17.100	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
122.114.17.100	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
85.250.64.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.247.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.50.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.179.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.104.41.54	147.237.76.198	Moldova, Republic of	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

11-22-2015-12:04:06 to 11-22-2015-13:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.178.123.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	600
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	134
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	84
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	61
31.168.17.161	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.52.17.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
37.26.146.187	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	26
2.52.185.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	24
100.100.81.226		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
31.168.85.158	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.214.11.209	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.180.154.125	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.19.85.114	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
84.111.46.196	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
31.168.85.156	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
213.57.131.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
31.186.228.93	United Kingdom	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.26.146.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
104.131.200.249	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.179.172.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.17	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.159	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	11
79.176.7.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.26.148.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
31.186.228.95	United Kingdom	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.15.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
37.140.141.37	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.52.9.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.22.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.189.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
31.186.228.57	United Kingdom	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
216.223.27.26	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
212.179.9.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.228.175	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
31.186.228.60	United Kingdom	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
173.252.115.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
173.252.81.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.113	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.123.32	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	307
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	245
109.67.100.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	237
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	231
46.19.85.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	175
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
109.67.100.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
109.67.100.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	75
46.19.86.17	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	72
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	72
37.26.146.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
109.67.100.245	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.67.100.245	Block	38
2.54.33.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
176.12.142.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
46.19.86.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	14
46.19.85.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
2.52.17.0	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	9
176.13.21.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.85.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.52.185.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.19.85.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.146.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
54.190.220.60	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 54.190.220.60	Block	4
176.13.22.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.48.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.140.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.228.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.8.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.102.169.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.71	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.3.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.102.215.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
5.102.254.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
37.236.228.30	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
176.13.10.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
54.190.220.60	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/navmenu/	Block	2
84.229.148.103	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	2
207.46.13.134	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
52.33.66.29	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 52.33.66.29	Block	2
2.52.26.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.80.131.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
176.13.15.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
83.130.110.22	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-22-2015-12:04:06 to 11-22-2015-13:04:06