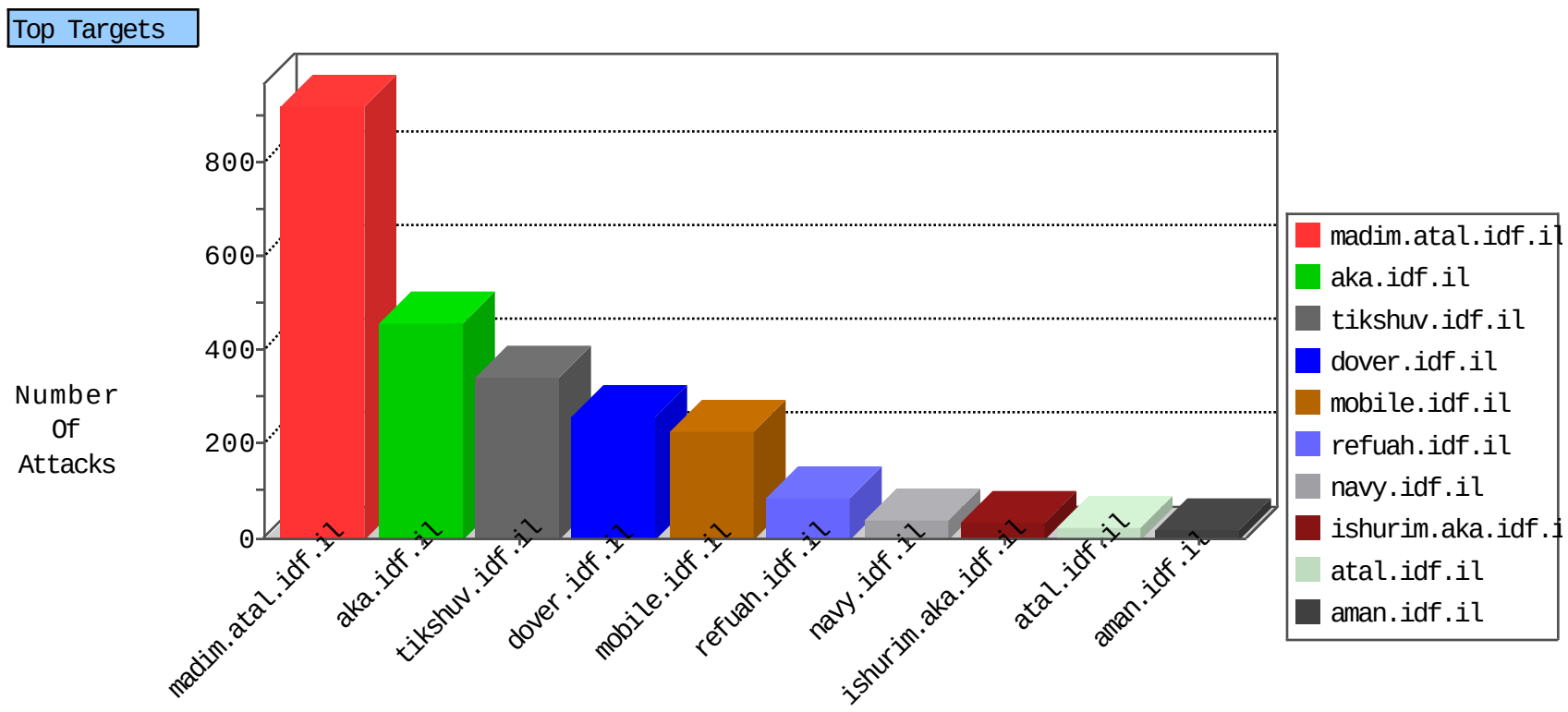
01-31-2016-12:04:04 to 01-31-2016-13:04:04

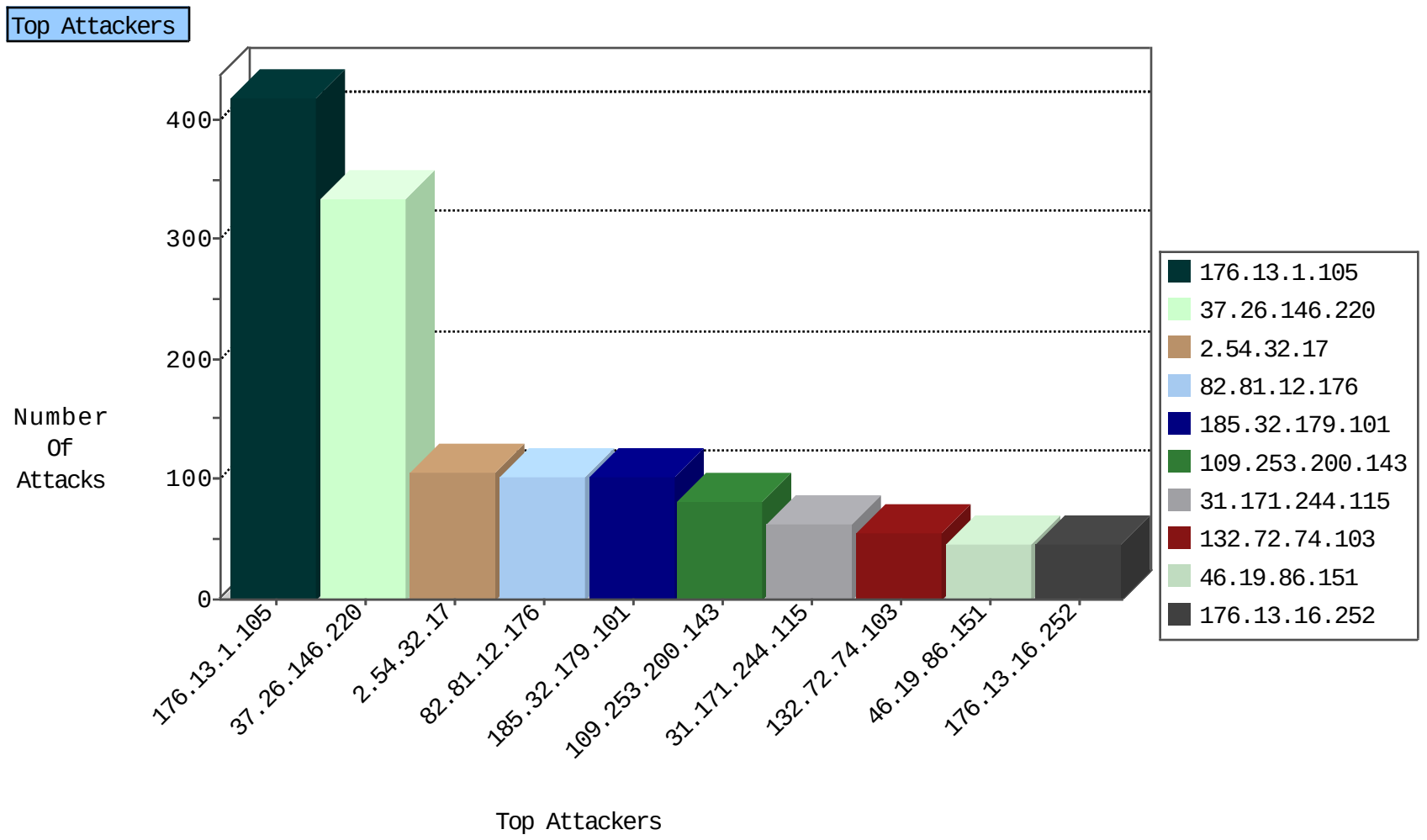
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-31-2016-12:04:04 to 01-31-2016-13:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	102
79.176.60.78	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.176.60.78	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.72.166	aka.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
74.91.28.62	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
146.185.239.100	Russian Federation	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1

01-31-2016-12:04:04 to 01-31-2016-13:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-31-2016-12:04:04 to 01-31-2016-13:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
52.34.40.182	147.237.77.170	United States	maarachot.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
213.8.46.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
27.124.121.194	147.237.76.44	Australia	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.115.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.87.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.248.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.37.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.223.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.54.250.114	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.170.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.48.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.129.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.61.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.117.157.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
8.37.237.222	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
192.117.141.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.153.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.40	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.187.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.146.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.198.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.157.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-31-2016-12:04:04 to 01-31-2016-13:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.220	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	335
31.171.244.115	Switzerland	147.237.77.216	dover.idf.il	drop	SAM rule	drop	62
132.72.74.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
217.132.138.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
109.253.150.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
176.13.14.66	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.132.126	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
154.121.5.233	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
185.127.10.37		147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
46.19.86.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
2.54.43.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.128.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.14.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
46.19.85.22	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.177.171.118	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
2.52.33.201	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.19.85.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.200.143	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
176.13.4.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.168.241.14	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.151	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
79.178.254.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.178.254.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.253.194.51	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.11.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.192	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.120.125.16		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.192	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.32.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.23.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	6
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.146.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.62.222	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.26.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.112	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.234.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.11.122	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.248	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.102	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.145.220.125	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.176.41.151	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
81.218.171.217	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5

01-31-2016-12:04:04 to 01-31-2016-13:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.1.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	248
176.13.1.105	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
185.32.179.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
2.54.32.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	77
176.13.1.105	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.1.105	Block	60
176.13.16.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
176.13.0.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
109.253.200.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	41
109.253.200.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
109.253.159.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.54.32.17	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	28
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
46.19.85.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
176.13.5.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
185.32.179.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	9
46.19.86.53	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.150.215	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.14.66	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
2.54.132.126	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
217.132.138.228	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.128.247	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.208.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.9.118	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.218.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.13.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.144.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.206.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.38	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.112	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
82.80.27.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1679-18967/dover.aspx	Block	2
81.218.97.114	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/2/size338x0/1802.jpg	Block	2
46.19.85.139	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
176.13.4.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.43.16	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.10.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.140.101	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
199.203.151.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
46.19.86.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.86	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.194.51	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
188.143.232.26	Russian Federation	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 188.143.232.26	Block	2
109.253.208.112	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
2.54.131.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
199.203.100.20	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
77.125.81.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
169.0.218.222		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
2.54.10.225	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1

01-31-2016-12:04:04 to 01-31-2016-13:04:04