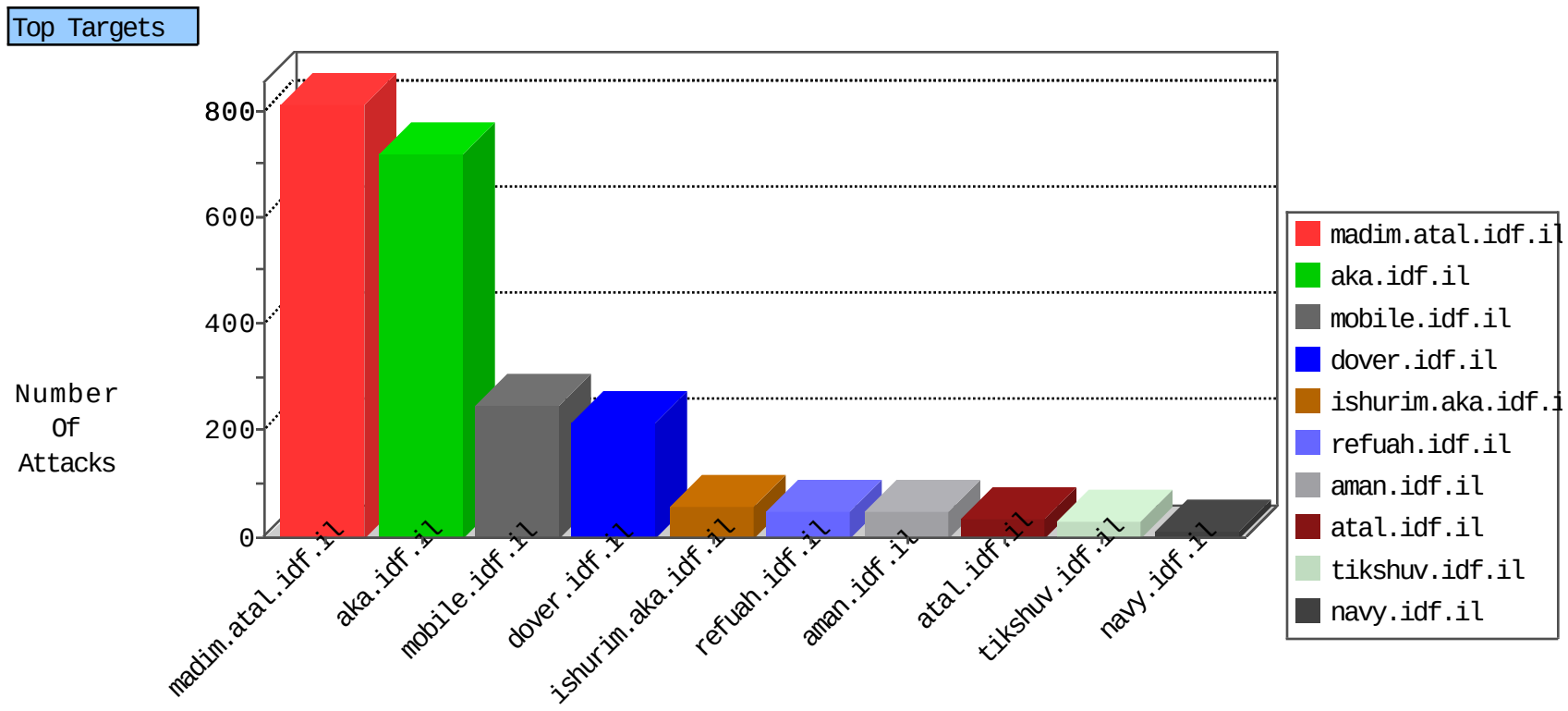
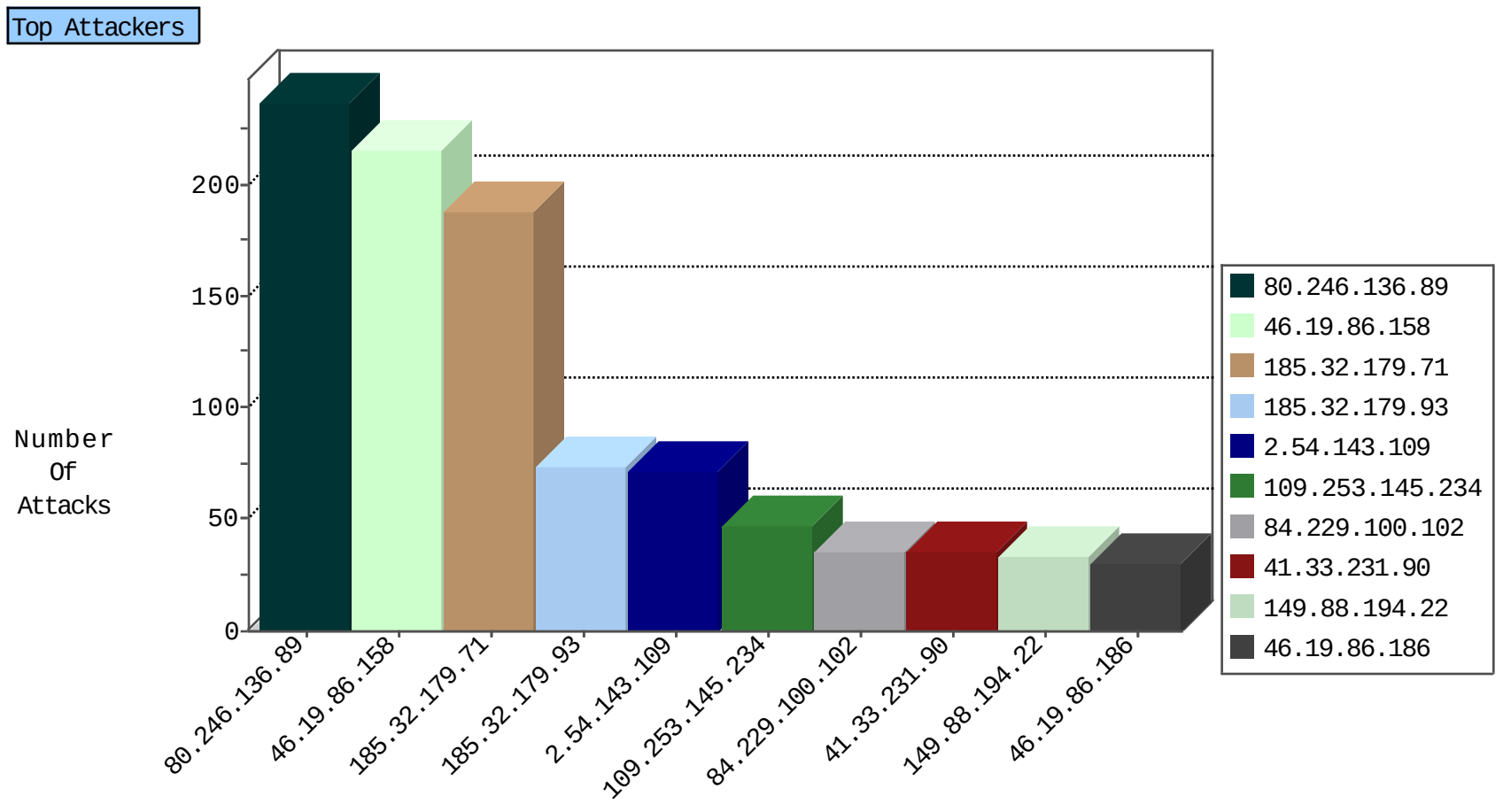
01-31-2016-19:04:02 to 01-31-2016-20:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



01-31-2016-19:04:02 to 01-31-2016-20:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	113
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
142.54.160.211	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
142.54.169.166	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
45.63.16.166		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
146.185.239.100	Russian Federation	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
74.91.28.61	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1

01-31-2016-19:04:02 to 01-31-2016-20:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.229.169.0	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

01-31-2016-19:04:02 to 01-31-2016-20:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.90.131.234	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
185.32.179.71	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
5.28.140.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.40.195.144	147.237.76.44	China	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
86.127.195.138	147.237.76.198	Romania	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
86.127.195.138	147.237.76.198	Romania	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
79.176.114.208	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
196.203.149.203	147.237.72.166	Tunisia	aka.idf.il	portscan: TCP Distributed Portscan	1
50.204.188.142	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.206.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.55.32.113	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.247.3	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.229.169.0	147.237.77.216	Turkey	dover.idf.il	SERVER-WEBAPP admin.php access	1
86.127.195.138	147.237.76.198	Romania	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
85.64.72.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.102.9.90	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
199.180.114.67	147.237.77.233	Poland	atal.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
185.32.179.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.252.84	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 3072	1

01-31-2016-19:04:02 to 01-31-2016-20:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.181.37.13	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
46.19.86.186	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	27
84.229.100.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
185.32.179.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	26
2.54.143.109	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	26
109.253.138.144	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
79.177.121.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.143.115	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.175.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
185.32.179.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
2.54.143.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
2.54.143.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.54.134.226	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.143.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
185.32.179.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.65.6.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.85.174	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
80.246.139.167	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.210.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.179.150.224	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.120.233.32	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
31.210.187.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.121.119.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
185.32.179.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	8
2.54.143.109	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.57	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.159.62	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.52.63.136	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	6
2.54.145.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.120.143.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.53.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.69.194.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.10.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.121.90.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.133.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.69.194.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.3.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.42.175	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
79.181.139.169	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
77.125.135.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.129.228	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
84.228.162.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.130.39	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.221.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

01-31-2016-19:04:02 to 01-31-2016-20:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	136
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	113
185.32.179.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
80.246.136.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	101
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	97
185.32.179.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	67
109.253.145.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
149.88.194.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
46.210.154.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
109.66.117.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/popups/markivsachar.aspx	None	13
46.19.86.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
176.13.0.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
185.32.179.71	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	9
5.29.102.254	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	8
85.64.89.168	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 85.64.89.168	Block	6
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	6
84.229.100.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
88.229.169.0	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 88.229.169.0	Block	5
37.26.149.171	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
109.253.193.32	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	5
88.229.169.0	Turkey	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	4
149.88.194.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
157.55.39.245	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/home/main/home/default.aspx	Block	4
2.54.24.89	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.210.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
176.13.4.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.88.194.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	3
88.229.169.0	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 88.229.169.0	Block	3
77.127.139.161	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
212.199.57.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.64.89.168	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
79.179.150.224	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
84.229.100.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
157.55.39.103	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/home/main/home/default.aspx	Block	3
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
2.54.134.226	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.138.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.20.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.102.224.178	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.78.175.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.121.119.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
77.127.182.167	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1560	Block	2
46.117.122.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.138.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
217.132.143.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.199.57.202	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 212.199.57.202	Block	2
85.65.122.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	2

01-31-2016-19:04:02 to 01-31-2016-20:04:02